(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－270785

(43)公開日　平成９年(1997)10月14日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/14			Ｈ０４Ｌ	9/00	６４１
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｂ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｂ

審査請求　未請求　請求項の数16　ＯＬ　（全 24 頁）

(21)出願番号　特願平8－180453

(22)出願日　平成８年(1996)７月10日

(31)優先権主張番号　特願平8－13939

(32)優先日　平８(1996)１月30日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　河野　健二
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　田口　正弘
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　齊藤　和雄
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

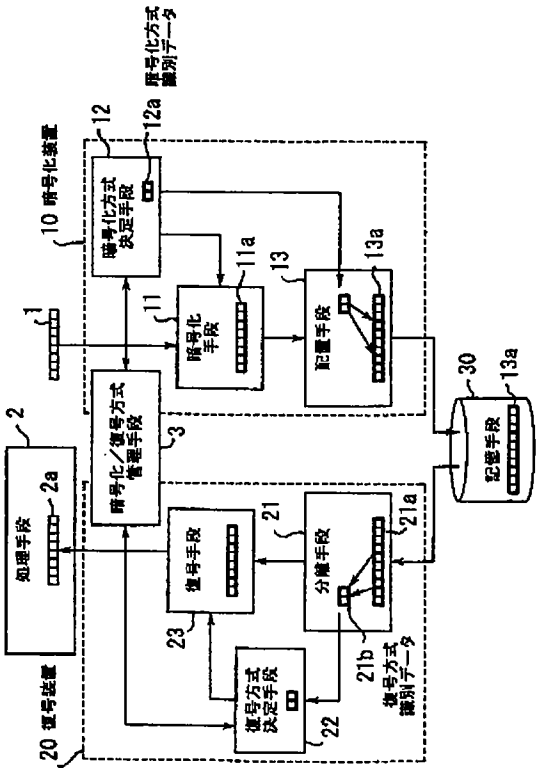
(74)代理人　弁理士　服部　毅巖

(54)【発明の名称】　情報処理装置

(57)【要約】

【課題】　コンピュータのメモリの管理方法に依存せずに、少ない計算量の暗号アルゴリズム及び簡単な鍵管理により暗号強度の高い暗号化データを得る。

【解決手段】　暗号化対象データ１は任意の暗号化方式により暗号化され暗号データ１１ａとなる。配置手段１３により、暗号化方式を示す暗号化方式識別データ１２ａが暗号データ１１ａ内に配置され、暗号データ１３ａが生成される。暗号データ１３ａは、記憶手段３０に格納される。暗号データ１３ａのデータ処理が必要になると、分離手段２１により、暗号データ１３ａが復号対象データ２１ａと復号方式識別データ２１ｂとに分離される。復号方式決定手段２２が、復号方式識別データ２１ｂから復号方式を決定し、その復号方式により復号手段２３が、復号対象データ２１ａを復号する。復号手段２３により復号されたデータ２ａは、暗号化対象データ１と同一のデータとなる。



【特許請求の範囲】

【請求項１】　入力されたデータを、識別データと暗号化対象データとに分離する分離手段と、
前記分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、
前記決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成する暗号化手段と、
前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。

【請求項２】　入力されたデータを暗号化する暗号化装置を有する報処理装置において、
暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を選択する選択手段と、
前記選択手段により選択された暗号化方式を用いて前記入力されたデータを暗号化し、暗号化データを生成する暗号化手段と、
前記暗号化手段により暗号化された暗号化データを、所定の関数に入力して関数値を計算する計算手段と、
前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記計算手段により得られた関数値に対応付けて格納する復号方式記憶手段と、
を有することを特徴とする情報処理装置。

【請求項３】　暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、
前記決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、
前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。

【請求項４】　前記暗号化手段を囲む包囲体に対して外部から物理的な作用を受けると、前記暗号化手段の処置機能を司るデータを消去する安全保護手段を、さらに有することを特徴とする請求項１、請求項２、又は請求項３のいずれか１項に記載の情報処理装置。

【請求項５】　前記決定手段により決定される暗号化方式を変更する変更手段をさらに有することを特徴とする請求項１、請求項２、又は請求項３のいずれか１項に記載の情報処理装置。

【請求項６】　識別データが復号対象データ内の所定の位置に配置された入力データを、前記識別データと前記復号対象データとに分離する分離手段と、
前記分離手段が分離した前記識別データに応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する決定手段と、
前記決定手段で決定された復号方式を用いて、前記復号対象データを前記復号対象データと同ビット数に復号する復号手段と、
前記識別データを、前記復号手段で復号されたデータ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。

【請求項７】　入力された暗号化データを復号する復号装置を有する情報処理装置において、
前記暗号化データを、所定の関数に入力して関数値を計算する計算手段と、
前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記関数値に対応づけて格納する復号方式記憶手段と、
前記計算手段により算出された関数値に対応する復号方式を前記復号方式記憶手段内から選択する復号方式選択手段と、
前記復号方式選択手段で選択された復号方式を用いて、前記暗号化データを復号する復号手段と、
を有することを特徴とする情報処理装置。

【請求項８】　前記復号手段を囲む包囲体に対して外部から物理的な作用を受けると、前記復号手段の処理機能を司るデータを消去する安全保護手段を、さらに有することを特徴とする請求項６又は請求項７のいずれか１項に記載の情報処理装置。

【請求項９】　前記決定手段により決定される復号方式を変更する変更手段を、さらに有することを特徴とする請求項６又は請求項７のいずれか１項に記載の情報処理装置。

【請求項１０】　データの暗号化及び暗号化データの復号を行う暗号化装置及び復号装置を有する情報処理装置において、
入力されたデータを、識別データと暗号化対象データとに分離する入力データ分離手段と、
前記入力データ分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、
前記暗号化方式決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成する暗号化手段と、
前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、
前記配置手段により前記識別データが配置された暗号化データを格納する記憶手段と、
前記記憶手段に格納された前記識別データが配置された暗号化データを、識別データと暗号化データとに分離する分離手段と、
前記分離手段により分離された識別データに応じて、暗号化方式に対応した復号鍵と復号アルゴリズムとの組み

合わせにより特定される復号方式を決定する復号方式決定手段と、
前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを前記暗号化データと同ビット数に復号する復号手段と、
前記復号方式決定手段による復号方式を示す識別データを、前記復号手段で復号されたデータ内の所定の位置に配置する再配置手段と、
前記復号手段により復号されたデータの処理を行う情報処理手段と、
を有することを特徴とする情報処理装置。
【請求項１１】　データの暗号化及び暗号化データの復号を行う暗号化復号装置を有する情報処理装置において、
暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を選択する暗号化方式選択手段と、
前記暗号化方式選択手段により選択された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、
前記暗号化手段により暗号化された暗号化データを、特定の関数に入力して関数値を計算する第１の計算手段と、
前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記第１の計算手段により得られた関数値に対応づけて格納する復号方式記憶手段と、
前記暗号化手段により暗号化された暗号化データを格納する記憶手段と、
前記記憶手段に格納された暗号化データを、特定の関数に入力して関数値を計算する第２の計算手段と、
前記第２の計算手段により算出された関数値に対応する復号方式を、前記復号方式記憶手段内から選択する復号方式選択手段と、
前記復号方式選択手段で選択された復号方式を用いて、前記暗号化データを復号する復号手段と、
前記復号手段により復号されたデータの処理を行う情報処理手段と、
を有することを特徴とする情報処理装置。
【請求項１２】　予め復号鍵と復号アルゴリズムとが特定されている暗号化データが入力されると、入力された暗号化データを復号する既知方式復号手段をさらに有し、
前記暗号化手段は、前記既知方式復号手段で復号されたデータも、暗号化対象データとして暗号化することを特徴とする請求項２、請求項３、請求項１０、又は請求項１１のいずれか１項に記載の情報処理装置。
【請求項１３】　入力された暗号化データが暗号化された際の暗号化方式と異なる暗号化方式により、前記復号手段が復号したデータを暗号化する別方式暗号化手段を、さらに有することを特徴とする請求項６、請求項７、請求項１０、又は請求項１１のいずれか１項に記載の情報処理装置。
【請求項１４】　入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、
前記決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化する暗号化手段と、
を有することを特徴とする情報処理装置。
【請求項１５】　復号対象データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する決定手段と、
前記決定手段で決定された復号方式を用いて、前記復号対象データを復号する復号手段と、
を有することを特徴とする情報処理装置。
【請求項１６】　入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、
前記暗号化方式決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、
前記暗号化手段により生成された前記暗号化データを格納する記憶手段と、
前記記憶手段内に格納された前記暗号化データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する復号方式決定手段と、
前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを復号する復号手段と、
を有することを特徴とする情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はソフトウェアの保護機能付情報処理装置に関し、特に処理が行われたデータを逐次暗号化する暗号化装置を有するか、処理を行うべき暗号化データを逐次復号する復号装置を有するか、あるいはそれらの双方を有する情報処理装置に関する。
【０００２】
【従来の技術】作成したプログラムやデータ（以下、特にことわりのない限りプログラムとデータとを含めて単に「データ」と呼ぶ）を流通させる場合、データを盗用や改ざんあるいは不正使用から保護する必要がある。これまでの保護手段としては、データをロム化したり、フロッピー等に記憶しコピープロテクトをかける等の方法がとられてきた。ところが、このような方法ではデータの内容を容易に読み出すことが可能であるためデータを完全に保護することはできない。
【０００３】また、データを暗号化して流通させ、復号鍵を持ったユーザのみがデータを復号して使用できるようにすることが可能である。ただし、この方法では復号

された後のプログラムまたはデータが無防備であり、そこがセキュリティホールとなり盗用や改ざん及び不正使用を許してしまう結果となる。

【０００４】これらの問題を解決する技術として、復号された後のプログラムまたはデータを不正に入手できないようにするために、データを暗号化しメモリ等に格納しておきそれを中央処理装置で実行する時に復号する方式が、特開平２－１５５０３４号の「セキュリティ機能付き情報処理装置」に示されている。この方式では、データを保護するために、情報処理装置内部に暗号化装置と復号装置とを設けており、これにより、ソフトウェアの保護を図っている。この情報処理装置について具体的に説明する。

【０００５】図１８は従来のソフトウェアの保護を図った情報処理装置のブロック図である。図１８に示した情報処理装置は、中央処理装置５１０、記憶装置５２３、入力装置５２１、出力装置５２２、及び鍵入力装置５２４を備えている。さらに、中央処理装置５１０は、内部に演算部５１１、制御部５１２、暗号化・復号部５１３、及び鍵格納部５１４を備えている。

【０００６】中央処理装置５１０は、情報処理装置の中心部分として機能し、データの演算や他の装置の制御等を行う。記憶装置５２３は、データが格納される装置であり、中央処理装置５１０からの制御によって中央処理装置５１０内の暗号化・復号部５１３とデータの授受を行う。

【０００７】入力装置５２１は、中央処理装置５１０からの制御で情報処理装置の外部からのデータを受け取る。出力装置５２２は、中央処理装置５１０からの制御で情報処理装置のデータを外部に出力する。鍵入力装置５２４は、中央処理装置５１０の暗号化や復号を行うのに必要な鍵をセットする。

【０００８】中央処理装置５１０内の演算部５１１は入力装置５２１や記憶装置５２３から与えられたデータに対して算術演算や論理演算を行う。制御部５１２は記憶装置５２３からの命令を解釈し情報処理装置全体の制御を行う。鍵格納部５１４は、鍵入力装置５２４がセットした鍵を格納する。暗号化・復号部５１３は記憶装置５２３と演算部５１１との間にあり、暗号化されている記憶装置５２３上の命令及びデータを、鍵格納部５１４内の鍵を用いて演算部５１１が解釈できるように復号するとともに、演算部５１１で演算された結果を記憶装置５２３に書き込む際に、鍵格納部５１４内の鍵を用いて暗号化し記憶装置５２３に格納する。

【０００９】このような構成により、記憶装置５２３に格納されるデータを常に暗号化しておくことができる。そのため、記憶装置５２３内のデータを盗用してもその内容を解釈することは困難となり、データの秘匿性を高めることができる。

【００１０】ところで、この様なソフトウェアの保護機能が付いた情報処理装置においては、暗号化して格納されたプログラムやデータを実行時に逐次復号して実行しなければならない。そのため、復号する際のオーバーヘッドを考慮して計算量が少ない比較的簡単なアルゴリズムの暗号化方式（例えばＸＯＲ等）を用いなければならず、結果として暗号強度が低くなるという問題がある。従って、比較的簡単なアルゴリズムの暗号化方式でも暗号強度を出来るだけ高める必要がある。

【００１１】そこで、情報処理装置ごとに暗号化の方法を変えて非公開にする努力がなされている。ただし、このような方法を用いるとデータの互換性が大きく失われてしまうという新たな問題が発生する。しかも、プログラム内の命令コードの出現頻度や暗号化されたプログラムと装置の動作の対応などから、暗号化アルゴリズムや暗号鍵が類推できるので、装置単位で見ると必ずしも暗号強度が高くなったとは言えない。

【００１２】このように、単に暗号化の方式を非公開にするだけでは十分な暗号強度が得られないため、少ない計算量で高い暗号強度を得られるような、他の手法がいくつか考えられている。その例を、以下に説明する。

【００１３】第１の例として、メモリのアドレス（エリア）ごとに暗号化アルゴリズムを変える方式がある。これは、特開昭６３－１８４８５３号公報「携帯可能電子装置」に開示されている。これには、複数のエリアに分割されたデータメモリ部と、このデータメモリ部に対してデータの読み出し及びデータの書き込みを行うための制御部とを設け、データメモリ部のエリアごとに異なる暗号化アルゴリズムが割当てられている。これにより、アドレスやエリアにより暗号化アルゴリズムや暗号鍵を変えることができ、データの秘匿性がより高いものとなる。

【００１４】第２の例として、メモリ内のあるアドレス上のデータによりそのデータ自身及び残りのデータ全てを暗号化する方式がある。これは、特開平４－２２９３４６号公報「プログラムコード保護用に使用すべきアドレスした情報のストリームのエンクリプション」に開示されている。この方式は、ＥＰＲＯＭ（Erasable andProgrammable Read Only Memory）内の保護されたプログラムまたはデータを開示することなしに検査または転送するためのものである。この方法によれば、暗号鍵がメモリ内のデータであるので暗号鍵を格納するキーバイトを特別に設ける必要がなく、ＥＰＲＯＭのシリコン面積を無駄に使用することがない。また、暗号鍵に用いたデータ領域も自身よって暗号化されるので、例えば暗号化方法に排他的ＮＯＲゲートを用いた場合には暗号鍵に用いたデータ領域が論理値１の出力バイトとなり暗号鍵を秘匿することができる。

【００１５】第３の例として、複数の暗号鍵を用いる代わりにＤＥＳ（Data Encryption Standard: 米商務省標準局〔現在の米国標準技術協会〕が１９７７年に公表し

た暗号アルゴリズム）の動作モードであるＣＢＣ（Cipher Block Chaining)やＣＦＢ（Cipher Feed Back）を用いて暗号強度を高める方式がある。これらは１つの暗号化ステップの出力を用いて次の暗号化ステップの入力を修正するものである。

【００１６】ＤＥＳは、暗号化の対象となるデータを６４ビットのブロックに分割し、１ブロックずつ処置するが、ＣＢＣでは、ブロック毎のデータと暗号鍵だけでなく、前のブロックの暗号化によって得られる値も使用する。一方、ＣＦＢは、最初のブロックを暗号化し、それによって得られた暗号化データをＤＥＳへの入力として使用して、擬似ランダム出力を生成する。この出力をさらに次のブロックのデータに結合し暗号文を生成する。これを繰り返し、暗号文を次々に連結していく。ＣＢＣやＣＦＢのようにすることでそれぞれの暗号ブロックは影響し合い、直前の暗号ブロックだけではなく全ての暗号ブロックを関連づけることができるので所与の順序以外では復号できないようにすることができる。

【００１７】第４の例として、特開平４－１０１５２９号公報「暗号化通信方式」が公開されている。これは、暗号化した電文中に暗号鍵を挿入して伝送し、受信された暗号化電文中から前記暗号鍵を抽出し、抽出された暗号鍵を使用して前記暗号化電文を解読することを特徴とする暗号化通信方式について記載したものである。この暗号化通信方式では、暗号鍵をそのまま暗号化電文中に挿入し、暗号鍵を挿入する位置は送信先との通信回数で決まる乱数値によって決定される。送信側と受信側では、お互いに通信回数をカウントするカウンタと、そのカウンタの値に応じた乱数値を発生させる乱数発生手段を共有している。この様にすることで、暗号鍵を通信ごとに変えることができ、盗聴者による盗聴を困難にすることができる。

【００１８】

【発明が解決しようとする課題】しかし、上記に示したような計算量が少なくかつ暗号強度を高めるための方式には、それぞれ次のような問題点がある。

【００１９】第１の例に示したアドレスやエリアにより暗号化アルゴリズムや暗号鍵を変える方法は、ＲＯＭ（Read Only Memory）のようなデータとデータアドレスの関係が変わらないようなメモリに対しては有効である。ところが、現在主流となっている仮想メモリを有するコンピュータには、この方法を適用することができない。

【００２０】つまり、仮想メモリを有するコンピュータでは、プロセッサに対して記憶装置がメインメモリと補助メモリとの階層構造をなしている。この場合、暗号化されたデータが補助メモリからメインメモリへスワップインしたり、メインメモリから補助メモリへスワップアウトするたびに暗号化されたデータのメインメモリ上のアドレスが頻繁に変化する。その結果、暗号化アルゴリズムまたは暗号鍵とデータアドレス上の暗号化されたデータとの整合が取れなくなるという問題が生じる。

【００２１】第２の例に示した方式は、暗号化の領域がアドレスにより決定されており、第１の例に示した方式と同様にメモリの階層構造を持った記憶装置には適用できない。

【００２２】第３の例に示した方式は、実質的には１つの暗号鍵しか用いていないので、その暗号鍵が露呈した場合には他の全てのデータが解読されてしまうという問題は解決されない。

【００２３】第４の例に示した方式は、通信に用いる暗号化方式であり、通信側と受信側で暗号鍵を共用しないですむように、暗号鍵そのものを暗号化電文中に挿入している。従って、暗号鍵を挿入する位置が盗聴者に知られてしまうと、暗号鍵そのものが露呈してしまうという問題が生じる。それを防ぐために第４の例では、通信回数で決まる乱数値によって暗号鍵を挿入する位置を変化させてこの問題を解消させていた。従って、通信側と受信側で正確にデータをやり取りするためには、互いに同期を取る必要があり、暗号化される順番と復号される順番を同じにする必要がある。しかし、ランダムアクセスを基本とした情報処理装置のメモリにおいて、上記の方式を適用することは事実上不可能である。

【００２４】また、情報処理装置で取り扱われるデータの単位は、処理の効率上同一のビット数（３２ビットや６４ビット）となることが多い。従って、暗号化することにより暗号鍵のビット数分データが付加されると、暗号化前と暗号化さた後とではデータのサイズが変化してしまうため、それを前提にしてソフトウェアを設計しなければならず、ソフトウェアの汎用性が大きく損なわれてしまうと共に、一部暗号化方式の情報をソフトウェア開発者に公開しなければならなくなり、暗号強度が著しく低下することになる。

【００２５】また、ソフトウェアの汎用性を保とうとすると、データのサイズの変化をハードウェアで補わなければならなくなり情報処理装置のアーキテクチャの大幅な設計変更が必要となる。

【００２６】さらに、情報処理装置で取り扱われるデータの単位は一般に通信の場合よりも短く、暗号化されるデータに対する暗号鍵データのサイズの割合が大きくなり記憶装置のメモリ空間を有効に活用できなくなるという問題が生じる。また、メモリ空間を浪費しないように暗号鍵データのサイズを短くすると、暗号強度が低下してしまう。

【００２７】なお、第１の例に示した方式の問題点を解決する手段として、アドレスやエリアを仮想メモリ空間に対応させることにより、暗号化アルゴリズムまたは暗号鍵とアドレス上の暗号化されたデータとの整合を取ることも可能である。ただし、このような仮想アドレスの管理はオペレーションシステム（以下、ＯＳと呼ぶ）で

行わなければならない。一般にＯＳはソフトウェアであるので、特に暗号強度が低いこのようなシステムでは、ＯＳ内の暗号化アルゴリズムまたは暗号鍵の切替えを制御している部分を集中的に解読することで容易に改ざん可能である。その結果、一旦装置内部で復号したデータをそのまま外部に出力するような改ざんが可能となり、ＯＳの一部を改ざんしただけで全てのデータが解読されるという問題が生じる。

【００２８】以上のように、従来は、コンピュータのメモリの管理方法に依存せずに、少ない計算量で高い暗号強度を得ることが困難であった。なお、複数の鍵又は暗号アルゴリズムを用いた暗号方法を用いれば、少ない計算で強い暗号強度が得られるが、この場合であっても、ＯＳの制御による複雑な鍵管理が介在しないことが条件である。

【００２９】本発明はこのような点に鑑みてなされたものであり、コンピュータのメモリの管理方法に依存せずに、少ない計算量の暗号アルゴリズム及び簡単な鍵管理により暗号強度の高い暗号化データを得る暗号化装置を有する情報処理装置を提供することを目的とする。

【００３０】また、本発明の他の目的は、コンピュータのメモリの管理方法に依存せずに、暗号強度の高い暗号化データを少ない計算量の復号アルゴリズム及び簡単な鍵管理で復号することができる復号装置を有する情報処理装置を提供することである。

【００３１】さらに、本発明の別の目的は、コンピュータのメモリの管理方法に依存せずに、暗号強度の高い暗号化データへの暗号化とその暗号化データの復号とを、少ない計算量の暗号化／復号アルゴリズム及び簡単な鍵管理で行うことのできる暗号化／復号装置を有する情報処理装置を提供することにある。

【００３２】

【課題を解決するための手段】上記課題を解決するために、第１の発明では、入力されたデータを、識別データと暗号化対象データとに分離する入力データ分離手段と、前記入力データ分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、前記暗号化方式決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、前記配置手段により前記識別データが配置された暗号化データを格納する記憶手段と、前記記憶手段に格納された前記識別データが配置された暗号化データを、識別データと暗号化データとに分離する分離手段と、前記分離手段により分離された識別データに応じて、復号鍵と復号アルゴリズムとの組み合わせにより特定される復号方式を決定する復号方式決定手段と、前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを復号する復号手段と、前記識別データを前記復号手段で復号されたデータ内の所定の位置に配置する再配置手段と、前記再配置手段により識別データが配置されたデータの処理を行う情報処理手段と、を有することを特徴とする情報処理装置が提供される。

【００３３】この情報処理装置によれば、暗号化されているデータが識別データと暗号化データとに分離され、分離された識別データにより暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。また、入力されたデータの一部を識別データとして用いているので、復号方式を特定するために余分な情報を付加する必要がない。また、暗号鍵そのものではなく識別データを用いることによって暗号鍵のビット長に制約がなくなるとともに、暗号化アルゴリズムも複数のものを使用することが可能となる。

【００３４】また、第２の発明では、暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、前記暗号化方式決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、前記暗号化手段により暗号化された暗号化データを、所定の関数に入力して関数値を計算する第１の計算手段と、前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記第１の計算手段により得られた関数値に対応づけて格納する復号方式記憶手段と、前記暗号化手段により暗号化された暗号化データを格納する記憶手段と、前記記憶手段に格納された暗号化データを、前記第１の計算手段で用いられた関数に入力して関数値を計算する第２の計算手段と、前記第２の計算手段により算出された関数値に対応する復号方式を前記復号方式記憶手段内から選択し、復号方式を決定する復号方式決定手段と、前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを復号する復号手段と、前記復号手段により復号されたデータの処理を行う情報処理手段と、を有することを特徴とする情報処理装置が提供される。

【００３５】この情報処理装置によれば、暗号化データの関数値により暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号化方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。

【００３６】また、第３の発明では、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、前記決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し暗号化データを生成する暗号化手段と、前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、を有することを特徴とする情報処理装置が提供される。

【００３７】前記第３の発明においては、課題で述べたように暗号化した場合にデータのサイズが増加してしまうためソフトウェアを一部書き換えるか又はアーキテクチャの設計変更が必要となるが、暗号鍵そのものでなく識別データを付加しているのでソフトウェア設計者に識別データのビット長を公開したとしても、暗号鍵そのもののビット長は秘密にすることができるので、暗号強度の低下を防ぐことができる。従って、この情報処理装置によれば、暗号化されているデータにより暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号化方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。また、暗号鍵そのものではなく識別データを用いることによって暗号鍵のビット長に制約がなくなるとともに、暗号化アルゴリズムも複数のものを使用することが可能となる。

【００３８】また、第４の発明では、入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、前記暗号化方式決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、前記暗号化手段により生成された前記暗号化データを格納する記憶手段と、前記記憶手段内に格納された前記暗号化データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する復号方式決定手段と、前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを復号する復号手段と、を有することを特徴とする情報処理装置が提供される。

【００３９】第４の発明の情報処理装置によれば、パリティビットの値により暗号化方式と復号方式を決定することができるため、メモリのエリアごとの管理やアドレスごとの管理がまったく必要なくなるとともに、汎用のパリティチェック機構を暗号化方式又は復号方式の決定に利用することで、複数の暗号化方式又は復号方式の管理に必要な機構を大幅に削減することができる。

【００４０】図１は本発明の情報処理装置の原理構成を示す図である。第１の発明では、暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段１２と、前記暗号化方式決定手段１２により決定された暗号化方式を用いて暗号化対象データ１を暗号化し、暗号データ１１ａを生成する暗号化手段１１と、前記暗号データ１の暗号化に用いられた暗号化方式を示す暗号化方式識別データ１２ａを、前記暗号データ内の所定の位置に配置する配置手段１３と、前記配置手段１３により暗号化方式識別データ１２ａが配置された暗号データ１３ａを格納する記憶手段３０と、前記記憶手段３０に格納された暗号データ１３ａを、復号方式識別データ２１ｂと復号対象データ２１ａとに分離する分離手段２１と、前記分離手段２１により分離された復号方式識別データ２１ｂに応じて、復号鍵と復号アルゴリズムとの組み合わせにより特定される復号方式を決定する復号方式決定手段２２と、前記復号方式決定手段２２で決定された復号方式を用いて、前記復号対象データ２１ａを復号する復号手段２３と、復号手段２３が復号したデータに含まれる命令に従って、復号したデータを処理する処理手段２と、暗号化方式決定手段１２及び復号方式決定手段２２で取り扱う暗号化方式と復号方式とを対応づける暗号化／復号方式管理手段３と、を有することを特徴とする情報処理装置が提供される。

【００４１】この情報処理装置によれば、暗号化対象データ１は任意の暗号化方式により暗号化され暗号データ１１ａとなる。さらに、暗号化方式を示す暗号化方式識別データ１２ａが暗号データ１１ａ内に配置された暗号データ１３ａが生成される。暗号データ１３ａは、記憶手段３０に格納される。そして、暗号データ１３ａのデータ処理が必要になると、分離手段２１により、暗号データ１３ａが復号対象データ２１ａと復号方式識別データ２１ｂとに分離される。そして、復号方式決定手段２２が、復号方式識別データ２１ｂから復号方式を決定し、その復号方式により復号手段２３が、復号対象データ２１ａを復号する。復号手段２３により復号されたデータ２ａは、暗号化対象データ１と同一のデータとなる。データ２ａは、自己に含まれた命令に基づき、処理手段２によって処理される。暗号化方式決定手段１２及び復号方式決定手段２２で取り扱う暗号鍵や復号鍵及び暗号化アルゴリズムや復号アルゴリズムは、暗号化／復号方式管理手段３で管理されており、識別データに対応した暗号鍵や復号鍵及び暗号化アルゴリズムや復号アルゴリズムが暗号化／復号方式管理手段３から供給される。

【００４２】このようにして、暗号データ内に識別データを含ませることによりコンピュータのメモリの管理方法に依存せずに、復号の際の復号アルゴリズムと復号鍵とを特定することができる。

【００４３】

【発明の実施の形態】以下、本発明の実施の形態を図面

に基づいて説明する。図１は本発明の情報処理装置の原理構成を示す図である。本発明の情報処理装置は、入力された暗号化対象データ１を暗号化する暗号化装置１０、処理を行うべきデータを復号して出力する復号装置２０、暗号化装置１０で暗号化された暗号化データ１３ａを格納しておく記憶手段３０、復号手段２３が復号したデータに含まれる命令に従って、復号したデータを処理する処理手段２、及び暗号化方式決定手段１２及び復号方式決定手段２２で取り扱う暗号化方式と復号方式とを対応づける暗号化／復号方式管理手段３から構成される。

【００４４】暗号化装置１０には、暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段１２と、暗号化方式決定手段１２により決定された暗号化方式を用いて暗号化対象データ１を暗号化し、暗号化データ１１ａを生成する暗号化手段１１と、暗号化データ１１ａの暗号化に用いられた暗号化方式を示す暗号化方式識別データ１２ａを、暗号化データ内の所定の位置に配置する配置手段１３とが設けられている。

【００４５】復号装置２０には、記憶手段３０に格納された暗号化データ１３ａを、復号対象データ２１ａと復号方式識別データ２１ｂとに分離する分離手段２１と、分離手段２１により分離された復号方式識別データ２１ｂに応じて、復号鍵と復号アルゴリズムとの組み合わせにより特定される復号方式を決定する復号方式決定手段２２と、復号方式決定手段２２で決定された復号方式を用いて、復号対象データ２１ａを復号する復号手段２３とが設けられている。

【００４６】この情報処理装置によれば、暗号化装置１０に暗号化対象データ１が入力されると、暗号化方式決定手段１２は暗号化方式識別データ１２ａを定め、その暗号化方式識別データ１２ａに応じた暗号鍵及び暗号化アルゴリズムが、暗号化／復号方式管理手段３から暗号化方式決定手段１２に供給される。暗号化方式決定手段１２は、暗号化対象データ１の暗号化方式を、暗号化／復号方式管理手段３から供給された暗号化方式に決定する。そして、暗号化対象データ１は、暗号化方式決定手段１２が決定した暗号化方式で、暗号化手段１１により暗号化され暗号化データ１１ａとなる。さらに、配置手段１３により、暗号化方式を示す識別データ１２ａが暗号化データ１１ａ内に配置され暗号化データ１３ａとなる。この暗号化データ１３ａは、記憶手段３０に格納される。これで、暗号化の処理は終了する。

【００４７】暗号化データ１３ａのデータ処理を行う要求が発生すると、復号装置２０内の分離手段２１が、記憶手段３０に格納されている暗号化データ１３ａを復号対象データ２１ａと復号方式識別データ２１ｂとに分離する。すると、復号方式決定手段２２は、暗号化／復号方式管理手段３から復号方式識別データ２１ｂに応じた復号鍵及び復号アルゴリズムの供給をうける。そして、復号方式決定手段２２は、復号対象データ２１ａの復号方式を、暗号化／復号方式管理手段３から供給された復号方式に決定する。復号対象データ２１ａは、復号方式決定手段２２で決定された復号方式で、復号手段２３により復号される。復号されたデータ２ａは、暗号化対象データ１と同じ内容のデータに戻っている。処理手段２は、復号されたデータ２ａに含まれる命令に従って処理を行う。

【００４８】これにより、暗号化方式は任意に定めることができるため、暗号化アルゴリズムと暗号鍵との組み合わせを複数用意し、暗号化対象データごとに異なる暗号化方式とすることができる。そのため、少ない計算量の暗号化アルゴリズムであっても暗号化強度の高い暗号化データを得ることができる。さらに、暗号化データ内に識別データを含ませることにより、復号の際には、コンピュータのメモリの管理方法に依存せずに復号方式を特定することができる。しかも、暗号化方式と復号方式とは、暗号化／復号方式管理手段３によって対応関係が管理されているため、もし暗号化データ内の識別データの位置が解読されたとしても、復号アルゴリズムや復号鍵が露呈することはなく、その暗号化データの復号方式を解読することはできない。

【００４９】図２は本発明を実施するソフトウェアの保護機能付き情報処理装置の概略構成を示すブロック図である。ソフトウェアの保護機能付き情報処理装置は、プログラムに従ってデータの処理を行うＭＰＵ（Micro Processing Unit）１１１と、ＭＰＵ１１１で取り扱われるデータの暗号化及び復号を行う暗号化／復号装置１１２と、暗号化／復号装置１１２で用いる暗号鍵及び復号鍵を格納する鍵テーブル１１３と、ＭＰＵ１１１によって処理されるデータを転送するためのシステムバス１３１と、暗号化／復号装置１１２で暗号化されたデータを格納するメインメモリ１２１と、Ｉ／Ｏインターフェース１２２と、Ｉ／Ｏインターフェース１２２を介して接続される補助メモリ１２３から構成されている。

【００５０】ここでは示していないがＭＰＵ１１１は内部にキャッシュメモリを含んでいる場合もある。また、メインメモリ１２１は主にＲＡＭ（Random Access Memory）等で構成される。補助メモリ１２３はハードディスク、フロッピーディスク、ＣＤ－ＲＯＭ等で構成される。暗号化／復号装置１１２は、暗号化及び復号のアルゴリズムは特定されており、暗号鍵と復号鍵が決まることにより、データの暗号化及び暗号化データの復号を実行することができる。

【００５１】図２に従ってソフトウェアの保護機能付き情報処理装置の動作を説明する。保護を受けるデータは、暗号化／復号装置１１２で暗号化された後に、メインメモリ１２１または補助メモリ１２３に格納される。この時、暗号化／復号装置１１２で用いる暗号化には複

数の暗号鍵が用意され、暗号鍵は暗号化されるデータの特定の数ビットを参照することにより鍵テーブル１１３から選択される。どのビットをどのように参照するか、その方法はソフトウェアの保護機能付き情報処理装置の各々に関して決定される。暗号化されたデータがＭＰＵ１１１で処理される時は、まず暗号化／復号装置１１２へ読み込まれ、ＭＰＵ１１１が処理を行えるように復号される。復号する時に用いられる復号鍵は、暗号化されているデータの特定の数ビットを参照することで、鍵テーブル１１３から選択される。この時の参照する数ビットを選ぶ方法は、前述の暗号鍵の選択の際に使用した方法との関係が一意であるように決定されている。ＭＰＵ１１１で処理されたデータが再びメインメモリ１２１または補助メモリ１２３に格納される時は、暗号化／復号装置１１２により再び暗号化される。以下、暗号化／復号装置１１２で行われる暗号化の詳細な説明を図３及び図４を用いて、また復号の詳細な説明を図５及び図６を用いて行う。

【００５２】図３は、図２に示される暗号化／復号装置１１２で用いられる暗号化方法のフローチャートを示す。このフローチャートの説明を行う。

［Ｓ１］暗号化されるべきデータを暗号化／復号装置１１２へ読み込む（ステップ１）。

［Ｓ２］暗号化／復号装置１１２において、読み込んだデータから特定の数ビットを抜き出す（ステップ２）。

［Ｓ３］ステップ２において抜き出した数ビットに対応する暗号鍵を、鍵テーブル１１３より選択する（ステップ３）。

［Ｓ４］ステップ３において選択した暗号鍵を用いて、暗号化されるべきデータの、抜き出した数ビット以外の部分を暗号化する（ステップ４）。

［Ｓ５］暗号化したデータに、ステップ２において抜き出した数ビットを埋め込む（ステップ５）。

【００５３】以上の各ステップにおいて、暗号化されるデータの状態がどのように変化するかを、図４の状態遷移図に従って説明する。なお、鍵テーブル１１３に格納される内容は、暗号化／復号方式ごと異なる。そこで、以後の説明において、鍵テーブル１１３の内容に言及する場合には、鍵テーブルには暗号化／復号方式ごとに個別の番号を付すこととするが、ハードウェアとしては図２に示す鍵テーブル１１３を指している。

【００５４】（Ａ）は、ステップ１の状態を示す図である。暗号化すべきデータ３１が読み込まれる。暗号化される前のデータ３１は３２ビットからなり、ＭＰＵ１１１で直接処理を行うことのできる状態にある。

【００５５】（Ｂ）は、ステップ２の状態を示す図である。暗号化される前のデータ３１から、特定の数ビットを抜き出す。例では７、１１、１５及び２３ビット目の４ビットのデータを抜き出している。従って、２８ビットのデータ３２が残ることとなる。抜き出したビットは、所定の配列に並べられビット情報３３となる。このビット情報３３は、図１に示す暗号化方式識別データ１２ａに対応する。（Ｃ）は、ステップ３の状態を示す図である。４ビットのビット情報３３に対応する暗号鍵を、予め用意された鍵テーブル４０から選択する。鍵テーブル４０は図２における鍵テーブル１１３にあたり、抜き出したビットによるビット情報４０ａに対応する鍵４０ｂが一意に選択できるようになっている。例では抜き出すビット数が４ビットであることから鍵も４ビットで分類されており、１６個のビット情報「００００」，「０００１」，「００１０」・・・のそれぞれに対応する１６個の鍵４１，４２，４３・・・が存在する。この例では、抜き出したビットによるビット情報３３の値が「００１０」であるため、鍵４３が暗号鍵として選択されている。

【００５６】（Ｄ）は、ステップ４の状態を示す図である。選択された鍵４３を暗号鍵に用いて、抜き出した４ビットのビット情報３３以外の２８ビットのデータ３２を暗号化し、２８ビットの暗号化データ３４を生成する。

【００５７】（Ｅ）は、ステップ５の状態を示す図である。（Ｂ）において抜き出した４ビットのビット情報３３を、２８ビットの暗号化データ３４に埋め込み、３２ビットの暗号化データ３５としてメインメモリ１２１に格納する。

【００５８】抜き出した４ビットのビット情報３３を埋め込む方法は、復号の際にビット情報３３を分離するための方法とセットで決定されている。この２つの方法が一意に決定できるのであれば、埋め込む位置を最初に抜き出したビット位置と同じにする必要はない。また、最後にスクランブル等を行い、第三者に暗号鍵の選択に用いたビットの位置を容易に見つけられないようにすることも可能である。なお、最後にスクランブルを行う場合には、ステップ４で行う暗号化はスクランブル以外の方法であることが望ましい。更に、抜き出した４ビットのビット情報３３を暗号化した２８ビットのデータ３４に埋めこむ際、ＸＯＲ等の暗号化方法で暗号化して埋めこんでもよい。

【００５９】図５には、図２に示される暗号化／復号装置１１２で用いられる復号方法のフローチャートを示す。このフローチャートの説明を行う。

［Ｓ１１］暗号化されているデータを暗号化／復号装置１１２へ読み込む（ステップ１１）。

［Ｓ１２］暗号化／復号装置１１２において、読み込んだデータから鍵の選択に用いた数ビットを抜き出す（ステップ１２）。

［Ｓ１３］ステップ１２において抜き出した数ビットに対応する復号鍵を、鍵テーブル１１３より選択する（ステップ１３）。

［Ｓ１４］ステップ１３において選択した復号鍵を用い

て、復号されるべきデータの、抜き出した数ビット以外の部分を復号する（ステップ１４）。

［Ｓ１５］復号したデータに、ステップ１２において抜き出した数ビットを埋め込む（ステップ１５）。

【００６０】復号されるデータの状態がどのように変化するかを、図６の状態遷移図に従って説明する。３２ビットのデータを復号する場合を考える。但しこの３２ビットのデータは、図３及び図４に示した暗号化方法に従って暗号化された後、メインメモリ１２１に格納されていたものとする。なお、この例は暗号鍵と同じ鍵を復号鍵とする場合である。

【００６１】（Ａ）は、ステップ１１の状態を示す図である。暗号化データ３５を記憶装置から読み込む。暗号化データ３５は３２ビットからなり、ＭＰＵ１１１で直接処理を行うことのできない状態にある。

【００６２】（Ｂ）は、ステップ１２の状態を示す図である。暗号化データ３５から、特定の数ビットを抜き出し、ビット情報３３を得る。例では６、１３、２７及び３０ビット目の４ビットを抜き出している。この４ビットのデータを抜き出す位置は、暗号化の際に、ビット情報３３の各ビットを埋め込んだ位置である。この結果、２８ビットの暗号化データ３４が残ることとなる。

【００６３】（Ｃ）は、ステップ１３の状態を示す図である。抜き出した４ビットのビット情報３３に対応する鍵４３を、予め用意された鍵テーブル４０から選択する。ビット情報３３の値は「００１０」であるため、鍵テーブル４０を用いて、暗号化の際の鍵４３と同一の鍵４３を選択することができる。この選択された鍵４３が復号鍵となる。

【００６４】（Ｄ）は、ステップ１４の状態を示す図である。選択した鍵４３を復号鍵として、抜き出した４ビットのビット情報３３以外の２８ビットの暗号化データ３４を復号し、２８ビットのデータ３２を生成する。

【００６５】（Ｅ）は、ステップ１５の状態を示す図である。（Ｂ）において抜き出した４ビットのビット情報３３を、２８ビットのデータ３２に埋め込み、３２ビットのデータ３１を得る。埋め込む位置は、暗号化の際に４ビットのデータを抜き出した位置と同じ位置である。この結果、暗号化する前のデータと同一のデータ３１が得られる。

【００６６】以上のような方法により、復号鍵の抽出に用いるデータが復号の対象となる暗号化されたデータの一部で構成される。そのため、余分な情報をデータに付加する必要がなく、メモリ空間を有効に使用できる。上記の例では具体的なビット数を示して説明を行ったが、これは説明を解りやすくするためであり、ビット数はソフトウェアの保護機能付き情報処理装置の各々で任意に選ぶことができる。従ってある単位、例えばバスで取り扱うビット単位（８ビット、１６ビット、３２ビット、６４ビット、１２８ビット等）や仮想記憶で用いられるページ単位、キャッシュメモリのデータを交換するビット単位等に関連させて暗号化のブロックを選択することで効率的な暗号化及び復号を行うことができる（このことは以下の説明においても同様である）。

【００６７】上記の例では、暗号化の鍵と復号の鍵とを選択する際に、同じ鍵テーブルを用いているため、暗号鍵と復号鍵が同一となっているが、暗号化の鍵テーブルと復号の鍵テーブルとを個別に設けることにより、暗号鍵と復号鍵とを個別のものにすることができる。これにより、暗号化の際に用いた暗号鍵と異なる復号鍵により復号するような暗号化／復号アルゴリズムを利用することもできる。

【００６８】また、上記の例では抜き出した数ビットから暗号鍵を選択する時に鍵テーブルを用いたが、抜き出した数ビットをある特定の関数に入力し、その出力値を暗号鍵として用いてもよく、そのようにすれば鍵テーブルを持つ必要がなくなる。勿論抜き出した特定の数ビットそのものを暗号鍵としてもよい。

【００６９】以上のような方法により、メインメモリ１２１または補助メモリ１２３に格納されたデータの内容を秘密にすることができる。また、暗号鍵及び復号鍵の選択がデータのみに依存しており、保護の対象であるデータの一部あるいは全部から暗号鍵を導出することができるため、特にアドレスに依存せずに、複数の暗号鍵でデータを暗号化することができる。その為、ＯＳによる複雑なアドレス管理が行われている場合でも、ＯＳに依存することなく複数の暗号鍵を管理することができる。つまり、ＯＳを改ざんすることにより秘匿データを盗用するという攻撃に対して、有効な防御を実現することができる。

【００７０】また、暗号化に複数の暗号鍵を使用しているので、計算量の少ない暗号化方法（例えばＸＯＲなど）を用いても十分な暗号強度を得ることができ、暗号化及び復号のプロセスがデータの処理速度に及ぼす影響を少なくすることができる。従って、メモリ中のデータを逐次復号しながらプログラムを実行する場合でも十分な実行速度と暗号強度を実現することができる。これにより、常にメインメモリ中に常駐するようなＯＳ自身を防御することも可能である。

【００７１】上記の例は、暗号化及び復号のアルゴリズムが一定であり、データごとに異なる暗号鍵と復号鍵とを使用した場合であるが、データごとに異なる暗号化及び復号のアルゴリズムを使用することもできる。図７は複数の暗号化及び復号のアルゴリズムを使用するソフトウェアの保護機能付き情報処理装置の概略構成を示すブロック図である。このソフトウェアの保護機能付き情報処理装置は、プログラムに従ってデータの処理を行うＭＰＵ（Micro Processing Unit）２１１と、ＭＰＵ２１１で取り扱われるデータの暗号化及び復号を行う暗号化／復号装置２１２と、暗号化／復号装置２１２で用いる

暗号化／復号のアルゴリズム及び暗号／復号鍵を格納する暗号化／復号アルゴリズム&鍵テーブル２１４と、ＭＰＵ２１１によって処理されるデータを転送するためのシステムバス２３１と、暗号化／復号装置２１２で暗号化されたデータを格納するメインメモリ２２１と、Ｉ／Ｏインターフェース２２２と、Ｉ／Ｏインターフェース２２２を介して接続される補助メモリ２２３から構成されている。

【００７２】ここでは示していないがＭＰＵ２１１は内部にキャッシュメモリを含んでいる場合もある。また、メインメモリ２２１は主にＲＡＭ等で構成される。補助メモリ２２３はハードディスク、フロッピーディスク、ＣＤ－ＲＯＭ等で構成される。暗号化／復号アルゴリズム&鍵テーブル２１４は、ＸＯＲやシフト等の複数種の暗号化アルゴリズム２１４ａと、各暗号化アルゴリズムに一意に対応する同数の復号アルゴリズム２１４ｂと、各暗号化アルゴリズムに一意に対応する同数の暗号鍵２１４ｃ、及び各復号アルゴリズム２１４ｂに一意に対応する同数の復号鍵２１４ｄを持つ。ここで、対応関係にある暗号化アルゴリズムと復号アルゴリズムとは、同じ方式のアルゴリズムである。

【００７３】この装置の動作は図２に示したソフトウェア保護機能付き情報処理装置とほぼ同様であるが、この例では暗号化される前のデータから抜き出す特定の数ビットを用いて、暗号化アルゴリズムの選択を行う。１つの暗号化アルゴリズムには、暗号鍵と、復号アルゴリズムと、復号鍵がそれぞれ１つずつ対応し、暗号化／復号アルゴリズム&鍵テーブル２１４に記憶されている。復号する場合は抜き出した特定の数ビットから復号アルゴリズム及び復号鍵を抽出して、データの復号を行う。

【００７４】このような方法で複数の暗号化／復号のアルゴリズムを用いてデータを暗号化することができ、更に暗号強度を高くすることができる。以上の２つの例では、いずれも暗号化の対象となるデータから抜き出されたビットを基に暗号鍵や暗号アルゴリズムを特定しているが、暗号鍵と暗号化対象データとの関連性は必ずしも必要ではない。そのため、任意の鍵を適当に選択して暗号鍵とすることもできる。なお、任意の鍵を適当に選択して暗号鍵とする場合の基本的なハードウェア構成については図２に示したソフトウェア保護機能付き情報処理装置と同じであり、暗号化／復号装置１１２の機能のみが異なる。そこで、適当に選択した鍵を暗号鍵とする場合の暗号化／復号装置の処理機能のみを、以下に説明する。

【００７５】図８は適当に選択した鍵を暗号鍵とする場合のフローチャートである。

［Ｓ２１］暗号化されるべきデータを暗号化／復号装置へ読み込む（ステップ２１）。

［Ｓ２２］暗号鍵を、鍵テーブルより任意に選択する（ステップ２２）。

［Ｓ２３］ステップ２２において選択した暗号鍵を用いて、暗号化されるべきデータ全てを暗号化する（ステップ２３）。

［Ｓ２４］暗号化されたデータに、ステップ２２において選択した暗号鍵のビット情報を埋め込む（ステップ２４）。

【００７６】次に、これらの各ステップにより、暗号化されるデータの状態がどのように変化するかを、図９の状態遷移図に従って説明する。ここでは、３２ビットのデータを暗号化する場合を考える。なお、図９における鍵テーブル６０は、図１における鍵テーブル１１３に相当する。鍵の長さとしては、例えば暗号化対象データと同じビット数、すなわち３２ビットを採用する。このように鍵のビット数も長くすること（できれば、暗号化対象データ長と同じビット数）によって、単に鍵を入力データから抽出した場合に比べ暗号化強度の向上が図れる。

【００７７】（Ａ）は、ステップ２１の状態を示す図である。暗号化される前のデータ５１は３２ビットからなり、ＭＰＵで直接処理を行うことのできる状態にある。（Ｂ）は、ステップ２２の状態を示す図である。鍵テーブル６０から任意に暗号鍵を選択し、対応するビット情報を調査する。鍵テーブル６０内の鍵６０ｂには、全て一意に定められた分類のためのビット情報６０ａが対応しており、図では４ビットの分類がされているので、合計１６個の鍵６１，６２，６３，・・・にビット情報「００００」，「０００１」，「００１０」・・・が対応付けられている。この例では、鍵６３が暗号鍵として選択されたものとする。鍵６３に対応するビット情報の値は「００１０」である。

【００７８】（Ｃ）は、ステップ２３の状態を示す図である。選択した鍵６３を暗号鍵に用いて、３２ビットのデータ５１を全て暗号化し、３２ビットの暗号化データ５２を生成する。

【００７９】（Ｄ）は、ステップ２４の状態を示す図である。（Ｂ）において調査したビット情報５３を、３２ビットの暗号化データ５２に埋め込み、３６ビットの暗号化データ５４として記憶装置に格納する。

【００８０】調査した情報ビット５３を埋め込む方法は、ソフトウェアの保護機能付き情報処理装置の各々によって、任意に決定される。暗号化データ５４を復号する場合は上記と逆のステップを行い、データ５１を得る。

【００８１】以上のような方法により、暗号鍵の選択をデータに依存せずに行うことができる。また復号鍵を選択する場合に鍵テーブルを用いず、ある特定の関数に抜き出した４ビットを入力すると復号鍵が得られるようにしてもよい。

【００８２】次に、暗号化データに暗号鍵の情報を埋め込むのではなく、ハッシュ関数を用いて暗号化データと

暗号鍵とを対応付けるソフトウェアの保護機能付き情報処理装置について説明する。

【００８３】図１０はハッシュ関数を用いて暗号化データと暗号鍵とを対応付ける場合のフローチャートである。これは、図２に示すソフトウェアの保護機能付き情報処理装置内部の、暗号化／復号装置１１２で用いる暗号化方法を変更したものの１つである。暗号化／復号装置以外の機能については図２に示すソフトウェアの保護機能付き情報処理装置と同じであるため、この例では、暗号化／復号装置の処理機能のみを説明する。

［Ｓ３１］暗号化されるべきデータを暗号化／復号装置１１２へ読み込む（ステップ３１）。

［Ｓ３２］暗号鍵を、鍵テーブル１１３より任意に選択する（ステップ３２）。

［Ｓ３３］ステップ３２において選択した暗号鍵を用いて、暗号化されるべきデータ全てを暗号化する（ステップ３３）。

［Ｓ３４］暗号化したデータのハッシュ値を計算する（ステップ３４）。

［Ｓ３５］ステップ３４において計算したハッシュ値と、暗号鍵をセットにしてハッシュテーブルに登録する（ステップ３５）。

【００８４】暗号化されるデータの状態がどのように変化するかを、図１１の状態遷移図に従って説明する。この例では、３２ビットのデータを暗号化する場合を考える。なお、図１１における鍵テーブル８０は、図２における鍵テーブル１１３に相当する。

【００８５】（Ａ）は、ステップ３１の状態を示す図である。暗号化される前のデータ７１は３２ビットからなり、ＭＰＵで直接処理を行うことのできる状態にある。（Ｂ）は、ステップ３２の状態を示す図である。鍵テーブル８０内の鍵８０ｂには、全て一意に定められた分類のためのビット情報８０ａが対応している。図では４ビットの分類がされているので、合計１６個の鍵８１，８２，８３，・・・にビット情報「００００」，「０００１」，「００１０」・・・が対応付けられている。この例では、鍵８３が暗号鍵として選択されたものとする。鍵８３に対応するビット情報の値は「００１０」である。

【００８６】（Ｃ）は、ステップ３３の状態を示す図である。選択した鍵８３を暗号鍵に用いて、３２ビットのデータ７１を全て暗号化し、３２ビットの暗号化データ７２を生成する。

【００８７】（Ｄ）は、ステップ３４の状態を示す図である。３２ビットの暗号化データ７２をハッシュ関数８４に入力して、ハッシュ値７３を得る。（Ｅ）は、ステップ３５の状態を示す図である。ハッシュ値７３と、暗号化に使用した鍵８３をセットにして、ハッシュテーブル９０に登録する。ハッシュテーブル９０はハッシュ値９０ａと鍵９０ｂとが各々一意に対応している。図では、ハッシュ値「０１０１０００１」、「０００１０１００」、「１００１０１１１」・・・に対応して鍵９１，９２，９３・・・が登録されている。３２ビットの暗号化データ７２は記憶装置に格納される。

【００８８】暗号化されたデータを復号する場合には、暗号化されたデータのハッシュ値を求めハッシュテーブルより鍵を抽出し、その鍵を復号鍵として復号を行う。以上のような手段により、暗号化されたデータのハッシュ値からハッシュテーブルを基に復号鍵を抽出できるので、ＯＳによる複雑なアドレス管理が行われている場合でもＯＳに依存することなく複数の暗号鍵を管理することができる。また、ハッシュ関数を用いることで、暗号化されるデータの膨大なデータ空間（この例では２３２ビット）をハッシュ値のデータ空間（この例では２８ビット）に圧縮することができるので、鍵の管理に用いるメモリ空間を小さくすることができる。

【００８９】なお、異なる２つのデータが、それぞれ異なる暗号鍵によって暗号化されたにも拘わらず同じハッシュ値を持つようになってしまった場合、１つのハッシュ値に対して暗号鍵が２つ存在することになり、どちらの暗号鍵を用いて暗号化したのか判らなくなることが考えられる。このような場合は、暗号化したデータのハッシュ値が、既に登録されているものと同じになった時点で、もう一度更に異なる暗号鍵で暗号化する等の処置をとることで問題を解決する。なお、この場合には、暗号化されたデータのハッシュ値が他のハッシュ値と同じでないことを確認するまで、暗号化前のデータをバッファ等に保持しておく必要がある。

【００９０】以上の例では、情報処理装置の内部で暗号化したデータを復号して実行する場合を想定しているが、これだけでは、この情報処理装置で使用するためのソフトウェアを、他の装置で開発することが難しくなってしまう。そこで、他の装置から提供されるデータを復号するための別の復号装置を新たに設けることにより、この問題に対処することができる。以下にその例を説明する。

【００９１】図１２は他の装置から提供される暗号化データを復号できるソフトウェアの保護機能付き情報処理装置を示すブロック図である。このソフトウェアの保護機能付き情報処理装置は、データの処理を行うＭＰＵ（Micro Processing Unit ）３１１と、暗号化されたデータの復号を行う復号装置３１２と、復号されたデータをすぐに暗号化する暗号化装置３１３と、暗号化装置３１３で暗号化されたデータを記憶するメインメモリ３２１と、暗号化装置３１３で暗号化され、メインメモリ３２１に記憶されているデータの復号を行う復号装置３１４と、システムバス３３１と、Ｉ／Ｏインターフェース（Ｉ／Ｏ）３２２と、補助メモリ３２３及びネットワーク３２５から構成されている。

【００９２】さらに、ＭＰＵ３１１、復号装置３１２、

暗号化装置３１３及び復号装置３１４は、外部からの観測またはプログラム及びデータの改ざんを防止する安全保護容器３１０内に格納されている。安全保護容器としては特開昭６３－１２４１５３号公報「記憶情報保護装置」に示されたようなものを用いることができる。この安全保護容器は、複雑な経路をたどる導体路が表面に形成された包囲体で秘密情報を取り扱う回路カードを囲み、内部の秘密情報を不正に解析しようとして包囲体を破壊した場合に導体路の切断や短絡が生じ、それをトリガーとして秘密情報を消去するという構造になっている。

【００９３】以上の構成において、まずデータは暗号化された状態で、ネットワーク３２５やＣＤ－ＲＯＭ等によってソフトウェア提供者からユーザに提供される。この時用いられる暗号化方式は汎用的で暗号強度の高いものである。例えば、ソフトウェア提供者は前記暗号化方式としてＤＥＳ（Data Encryption Standard）等を用いてユーザに提供するデータを暗号化する。そして暗号鍵は例えばＲＳＡ（Rivest Shamir Adleman ：Ronald Rivest, Adi Shamir, Leonard Adlemanの３氏が考案したアルゴリズム）暗号によってソフトウェアの保護機能付き情報処理装置の公開鍵で暗号化され、暗号化されたデータとペアにしてユーザに提供される。ユーザは、ＤＥＳを用いて暗号化されたデータをＩ／Ｏ３２２を介して復号装置３１２に送る。

【００９４】復号装置３１２で復号されたデータは、直接暗号化装置３１３に送られソフトウェアの保護機能付き情報処理装置各々に固有の非公開の暗号化アルゴリズム及び暗号鍵で暗号化される。この際の暗号化アルゴリズム及び暗号鍵を特定するための識別情報は、暗号化されたデータ内の所定の位置に埋め込まれるか、あるいは、暗号化されたデータのハッシュ値に対応付けて管理される。暗号化装置３１３で暗号化されたデータはメインメモリ３２１に格納される。

【００９５】ＭＰＵ３１１はメインメモリ３２１に格納されている暗号化されたデータを復号装置３１４で復号して受け取り、実行する。復号装置３１４が復号を行う際の復号鍵及び復号アルゴリズムは、暗号化データに埋め込まれた識別情報を解析するか、あるいは暗号化データのハッシュ値から求めることができる。ＭＰＵ３１１が処理を終了し出力するデータの中で暗号化が必要なものは、暗号装置３１３で暗号化されてからメインメモリ３２１に格納される。

【００９６】以上のように、公開された暗号方式と暗号鍵を用い暗号化されたデータを、ソフトウェアの保護機能付き情報処理装置内に取り込んで復号装置３１２で復号できるので、ソフトウェアの供者は暗号化装置３１３及び復号装置３１４で使用する暗号化／復号方式または暗号／復号鍵を知る必要はなく、ただＭＰＵ３１１用にソフトウェアの開発すればよい。つまり、ソフトウェアの保護機能付き情報処理装置内の暗号化／復号方式または暗号／復号鍵を知りえない第三者が、ソフトウェアの保護機能付き情報処理装置に守られるソフトウェアの自由に開発できる。また、復号されたデータは直接暗号化されるので、ユーザが復号されたデータにアクセスすることはできない。

【００９７】暗号化装置３１３及び復号装置３１４で用いられる暗号化方法及び復号方法に、前の例で示したように、アルゴリズムと鍵とを特定する識別情報を暗号化データに埋め込んだり、あるいはハッシュ値と識別情報を対応付ける方法を用いることにより、暗号化に複数の暗号鍵を使用できる。これにより、計算量の少ない暗号化アルゴリズムを利用しても十分な暗号強度を得ることができる。その結果、暗号化及び復号のプロセスがデータの処理速度に及ぼす影響を小さくすることができ、メモリ中のデータを逐次復号しながらプログラムを実行する場合でも、十分な実行速度と暗号強度を実現できる。

【００９８】また、暗号化装置３１３及び復号装置３１４で用いられる暗号化方法及び復号方法は、他の情報処理装置と共有する必要がないので、暗号化及び復号のアルゴリズムや暗号鍵及び復号鍵を、１つの情報処理装置内だけで独自に設定または更新することが可能である。ある条件（例えば電源オン／オフや１日ごと）で暗号化及び復号のアルゴリズムや暗号鍵及び復号鍵を更新するようにすれば、さらに暗号強度を高めることができる。電源オン／オフ時に暗号鍵及び復号鍵を更新するには、図２に示した鍵テーブル内の鍵の値を電源オン時に変更すればよい。

【００９９】また、ＭＰＵ３１１、復号装置３１２、暗号化装置３１３及び復号装置３１４が安全保護容器３１０内に格納されているため、内部の秘密情報を不正に解析しようとすると、安全保護容器３１０の包囲体が破壊され、秘密情報が消去される。その結果、暗号鍵、復号鍵及び暗号化されていないデータ等を取り扱うＭＰＵ、暗号化装置及び復号装置を安全保護容器内に格納すれば、不正を行おうとする者は暗号を解読する手掛かりをほとんど失うことになり、プログラム及びデータの秘匿性が、さらに高められる。

【０１００】ところで、図１２で示した例は他の装置で開発されたソフトウェアを受け取るための情報処理装置であるが、逆に、自己の内部で開発したソフトウェアを他の装置へ暗号化して送信する場合には、別の暗号化装置を新たに設ける。この暗号化装置では、ＤＥＳ等の暗号強度の高い暗号アルゴリズムで暗号化を行う。これにより、開発途中のソフトウェアは、計算量の少ないアルゴリズムと複数の鍵を組み合わせることにより暗号強度を高め、ソフトウェアを他の装置へ送信する際には、暗号強度の高いアルゴリズムを用いて暗号強度を高めることができる。

【０１０１】なお、以上の本発明の説明ではＭＰＵやメ

インメモリ 等の現在コンピュータシステムで使われている用語を用いたが、これらの用語は本発明をなんら限定するものではなく同等の機能を有するものであればよい。また、計算量の少ない暗号化及び復号アルゴリズムとして、ＸＯＲ、シフト及びスクランブル等を例にして述べてきたが、これらはコンピュータの処理能力が向上してくれば、さらに複雑な暗号化及び復号アルゴリズムと置き換えることが可能である。

【０１０２】図１３は本発明の情報処理装置の他の実施形態を示す図である。図１３において、３４０はネットワーク等から暗号化された情報を取り込み記憶する記憶装置を表す。３５０は記憶手段３４０に格納されている暗号化された情報を復号し、処理装置３６０が処理できるように復号する復号装置を表す。復号装置３５０には分離手段３５１、復号方式決定手段３５２、復号手段３５３、復号方式管理手段３５４、及び再配置手段３５５が含まれており、これらにより記憶装置３４０内に格納された暗号化されたデータ３４１の復号を行う。処理装置３６０は復号装置３５０により復号されたデータに基づいて処理を行う。図１３の装置の動作を以下に説明する。

【０１０３】記憶装置３４０は、ネットワークやＣＤ－ＲＯＭ等から暗号化されたデータを取り込み格納する。記憶装置３４０に格納されたデータ３４１は、復号装置３５０内の分離手段３５１に読み込まれ復号対象データ３５１ａと認識データ３５１ｂとに分離される。そして、復号対象データ３５１ａは復号手段３５３に読み込まれ、認識データ３５１ｂは復号方式決定手段３５２に読み込まれる。復号方式決定手段３５２は認識データ３５１ｂに対応した復号方式を復号方式管理手段３５４から選択し、復号アルゴリズム又は復号鍵を復号手段３５３に与える。復号手段３５３は与えられた復号アルゴリズム又は復号鍵を用いて復号対象データ３５１ａを復号する。復号手段３５３で復号されたデータと認識データ３５１ｂは再配置手段３５５により結合され、処理装置３６０で取り扱うことのできるデータ３６１となり、処理装置３６０により処理される。

【０１０４】このように、本発明の実施形態には復号装置のみを有する構成も考えられ、暗号化された情報は、予め復号方式管理手段３５４に保持されている復号方法と対応した暗号化方法を用いて暗号化されてネットワークやＣＤ－ＲＯＭ等で提供される。この装置構成が適用される領域としては、与えられた情報を変更する必要のない家庭用ゲーム機器や電子出版物等が挙げられる。また、これらの装置で取り扱う情報を暗号化する装置は、暗号化装置のみを有する構成となる。

【０１０５】また、暗号化すべきデータから抜き出すべき数ビットとして、パリティビットを用いることもできる。その例を以下に示す。この場合のハードウェア構成は、図２に示した制御装置と同様の構成であるため、図２の構成を用いて説明する。

【０１０６】図１４は、パリティビットにより鍵を特定する暗号化方法のフローチャートである。以下に、このフローチャートの説明を行う。ここでは、暗号化されていない３２ビットデータを４組で、暗号化の１単位とした場合を考える。

［Ｓ４１］暗号化／復号装置１１２は、暗号化されていない４組の３２ビットデータを読み込む（ステップ４１）。

［Ｓ４２］暗号化／復号装置１１２において、３２ビットデータごとのパリティビットを算出し、暗号鍵の選択に用いる４ビットを得る（ステップ４２）。

［Ｓ４３］ステップ４２において算出した４ビットに対応する暗号鍵を、予め用意している鍵テーブル１１３から選択する。それぞれの暗号鍵は４ビットで分類されており、この場合、合計１６個の暗号化鍵が存在する（ステップ４３）。

［Ｓ４４］ステップ４３において選択した暗号鍵を用いて、入力データを暗号化する（ステップ４４）。この際、パリティビットの値が変化しないような暗号化方式を用いる。例えば、スクランブルや置換等である。

［Ｓ４５］算出した４ビットをパリティビットとして暗号化したデータに付加してメインメモリ１２１又は補助メモリ１２３に格納する（ステップ４５）。

【０１０７】以上の各ステップにおいて、暗号化されるデータがどのように変化するかを、図１５の状態遷移図に従って説明する。この図において、鍵テーブル４１０は図２の鍵テーブル１１３の内容を示すものである。

【０１０８】（Ａ）は、ステップ４１の状態を示す図である。暗号化すべきデータ４０１が読み込まれる。暗号化される前のデータ４０１は、３２ビットのデータが４つで１単位である。

【０１０９】（Ｂ）は、ステップ４２の状態を示す図である。暗号化される前のデータ４０１から、３２ビットのデータごとのパリティビットを求める。求められたパリティビットが所定の配列に並べられ、４ビットのビット情報４０２となる。

【０１１０】（Ｃ）は、ステップ４３の状態を示す図である。４ビットのビット情報４０２に対応する暗号鍵を、予め用意された鍵テーブル４１０から選択する。鍵テーブル４１０は図２における鍵テーブル１１３にあたり、ステップ４２で抜き出したビット情報４０２に対応する鍵４１３が一意に選択できる。この例では抜き出すビット数が４ビットであることから鍵も４ビットで分類されており、１６個のビット情報「００００」，「０００１」，「００１０」・・・のそれぞれに対応する１６個の鍵４１１，４１２，４１３・・・が存在する。この図では、ビット情報４０２の値「００１０」に対応する鍵４１３が暗号鍵として選択される。

【０１１１】（Ｄ）は、ステップ４４の状態を示す図で

ある。選択された鍵４１３を暗号鍵に用いて、３２ビット×４のデータ４０１を暗号化し、暗号化データ４０３を生成する。なお、この際の暗号化方式は、パリティビットの値が変化しないような暗号化方式である。

【０１１２】（Ｅ）は、ステップ４５の状態を示す図である。（Ｂ）において算出した４ビットのビット情報４０２を、暗号化データ４０３のパリティビットとして付加し、パリティビット付きの暗号化データ４０４がメインメモリ１２１に格納される。

【０１１３】図１６はパリティビットにより鍵を特定する復号方法のフローチャートである。

［Ｓ５１］１組として暗号化されているデータ４０４を暗号化／復号装置１１２へ読み込む（ステップ５１）。

［Ｓ５２］暗号化／復号装置１１２において、読み込んだデータからパリティビットを抜き出し、復号鍵の選択に用いる４ビットのビット情報４０２を得る（ステップ５２）。

［Ｓ５３］ステップ５２において抜き出したビット情報４０２に対応する復号鍵４１３を、鍵テーブル４１０より選択する（ステップ５３）。

［Ｓ５４］ステップ５３において選択した復号鍵４１３を用いて、復号されるべきデータ４０４の、パリティビット以外の部分を復号する（ステップ５４）。

【０１１４】図１７は図１６の各ステップの状態遷移図である。なお、この例は暗号鍵と同じ鍵を復号鍵とする場合である。（Ａ）は、ステップ５１の状態を示す図である。暗号化データ４０４を記憶装置から読み込む。暗号化データ４０４は３２ビット×４のデータとパリティビットからなり、ＭＰＵ１１１で直接処理を行うことのできない状態にある。

【０１１５】（Ｂ）は、ステップ５２の状態を示す図である。暗号化データ４０４から、パリティビットを抜き出し、ビット情報４０２を得る。この結果、暗号化データ４０３が残ることとなる。

【０１１６】（Ｃ）は、ステップ５３の状態を示す図である。抜き出した４ビットのビット情報４０２に対応する鍵４１３を、予め用意された鍵テーブル４１０から選択する。ビット情報４０２の値は「００１０」であるため、鍵テーブル４１０を用いて、暗号化の際の鍵と同一の鍵４１３を選択することができる。

【０１１７】（Ｄ）は、ステップ５４の状態を示す図である。選択した鍵４１３を復号鍵として、抜き出した４ビットのビット情報４０２以外の暗号化データ４０３を復号し、３２ビット×４のデータ４０１を生成する。

【０１１８】なお、以上の説明で具体的なビット数が示したが、これは説明を分かりやすくするためであり、ビット数を任意に選ぶことができることは、図３～図６で示した暗号化／復号方法と同様である。即ち、例えばバスで取り扱うビット単位（８ビット、１６ビット、３２ビット、６４ビット、１２８ビット等）や仮想記憶で用いられるページ単位やキャッシュメモリのライン（ブロック）単位等に関連させて暗号化のブロックを選択することで効率的な暗号化及び復号を行うことができる。

【０１１９】パリティビットを用いて鍵を選択する場合も、図３～図６で示した暗号化／復号方法と同様の効果を有しており、ＯＳを介在させずに、計算量の少ない暗号化／復号方法を用いても十分な暗号強度を得ることがでる。しかも、このパリティビットを用いて鍵を選択する方法では、暗号鍵及び復号鍵の選択に用いるビットを抽出する機構として一般のコンピュータシステムに標準的に用いられているパリティチェックの機構を利用している。そのため、その部分の機構を装置に新たに付加する必要がなく、装置構成を簡単にすることができる。

【０１２０】なお、パリティビットにより鍵を選択する場合においても、図７に示したように、鍵テーブル１１３を暗号化／復号アルゴリズム&鍵テーブル２１４に置き換えることにより、鍵と暗号化／復号のアルゴリズムとの組み合わせを選択することも可能である。このようにすることで複数の暗号化／復号のアルゴリズムを用いてプログラムやデータを暗号化することができ、計算量の少ない暗号化方式においても暗号強度を十分高くすることができる。

【０１２１】

【発明の効果】以上説明したように、情報処理装置に係る第１の発明では、暗号化されたデータそのものが識別データと暗号化対象データとに分離され、分離された識別データにより暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。。従って、情報処理装置で取り扱われるデータを複数の暗号方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。また、暗号化されるデータの一部を識別データとして用いているので、復号方式を特定するために余分な情報を付加する必要がなく、データサイズが増加することによる複雑なアドレス管理やメモリの浪費を避けることができ、一般のコンピュータシステムに適用する場合に極めて有効である。また、識別データの位置が解析され識別データが露呈した場合でも暗号方式そのものが露呈することはなく、識別データの位置を固定とした場合でも暗号強度を十分強く保つことが可能である。これにより、暗号化データに対するランダムアクセスが可能となる。

【０１２２】また、情報処理装置に係る第２の発明では、暗号化データの関数値により暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号化方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合で

も暗号化強度の高い暗号化データを得ることができる。また、暗号化データに対するランダムアクセスも可能となる。

【０１２３】また、情報処理装置に係る第３の発明では、暗号鍵そのものではなく識別データを付加しているのでソフトウェア設計者に識別データのビット長を公開したとしても、暗号鍵そのもののビット長は秘密にすることができるので、暗号強度の低下を防ぐことができる。従って、この情報処理装置によれば、暗号化されているデータにより暗号化データの復号方式を特定することができるため、暗号化データの復号方式をコンピュータのメモリ管理方法に依存せずに特定することができる。従って、情報処理装置で取り扱われるデータを複数の暗号化方式で暗号化することが可能となり、計算量の少ない暗号化アルゴリズムを用いた場合でも暗号化強度の高い暗号化データを得ることができる。また、暗号鍵そのものではなく識別データを用いることによって暗号鍵のビット長に制約がなくなる。また、識別データの位置が解析され識別データが露呈した場合でも暗号方式そのものが露呈することはなく、識別データの位置を固定とした場合でも暗号強度を十分強く保つことが可能である。これにより暗号化データに対するランダムアクセスが可能となる。

【０１２４】また、情報処理装置に係る第４の発明では、データのパリティビットをもとに暗号化方式又は復号方式を決定するので、プログラムやデータを複数の暗号化方式又は復号方式で暗号化して一つのメモリに格納しても、メモリのエリアごとの管理やアドレスごとの管理がまったく必要なくなるとともに、汎用のパリティチェック機構を暗号化方式又は復号方式の決定に利用することで、複数の暗号化方式又は復号方式の管理に必要な機構を大幅に削減することができる。従って大幅なコスト低減が可能となる。

【図面の簡単な説明】

【図１】本発明の暗号化復号装置の原理構成を示す図である。

【図２】本発明を実施するソフトウェアの保護機能付き情報処理装置の概略構成を示すブロック図である。

【図３】図２に示される暗号化／復号装置の暗号化の処理手順を示すフローチャートである。

【図４】図３の各ステップの状態遷移を示す図である。（Ａ）はステップ１の状態を示す図であり、（Ｂ）はステップ２の状態を示す図であり、（Ｃ）はステップ３の状態を示す図であり、（Ｄ）はステップ４の状態を示す図であり、（Ｅ）はステップ５の状態を示す図である。

【図５】図２に示される暗号化／復号装置の復号の処理手順を示すフローチャートである。

【図６】図５の各ステップの状態遷移を示す図である。（Ａ）はステップ１１の状態を示す図であり、（Ｂ）はステップ１２の状態を示す図であり、（Ｃ）はステップ１３の状態を示す図であり、（Ｄ）はステップ１４の状態を示す図であり、（Ｅ）はステップ１５の状態を示す図である。

【図７】複数の暗号化及び復号のアルゴリズムを使用するソフトウェアの保護機能付き情報処理装置の概略構成を示すブロック図である。

【図８】適当に選択した鍵を暗号鍵とする場合の処理手順を示すフローチャートである。

【図９】図８の各ステップの状態遷移を示す図である。（Ａ）はステップ２１の状態を示す図であり、（Ｂ）はステップ２２の状態を示す図であり、（Ｃ）はステップ２３の状態を示す図であり、（Ｄ）はステップ２４の状態を示す図である。

【図１０】ハッシュ関数を用いて暗号化データと暗号鍵とを対応付ける場合の処理手順を示すフローチャートである。

【図１１】図１０の各ステップの状態遷移を示す図である。（Ａ）はステップ３１の状態を示す図であり、（Ｂ）はステップ３２の状態を示す図であり、（Ｃ）はステップ３３の状態を示す図であり、（Ｄ）はステップ３４の状態を示す図であり、（Ｅ）はステップ３５の状態を示す図である。

【図１２】他の装置から提供される暗号化データを復号できるソフトウェアの保護機能付き情報処理装置を示すブロック図である。

【図１３】本発明の情報処理装置の他の実施形態を示す図である。

【図１４】パリティビットにより鍵を特定する暗号化方法のフローチャートである。

【図１５】図１４の各ステップの状態遷移図である。（Ａ）はステップ４１の状態を示す図であり、（Ｂ）はステップ４２の状態を示す図であり、（Ｃ）はステップ４３の状態を示す図であり、（Ｄ）はステップ４４の状態を示す図であり、（Ｅ）はステップ４５の状態を示す図である。

【図１６】パリティビットにより鍵を特定する復号方法のフローチャートである。

【図１７】図１６の各ステップの状態遷移図である。（Ａ）はステップ５１の状態を示す図であり、（Ｂ）は、ステップ５２の状態を示す図であり、（Ｃ）はステップ５３の状態を示す図であり、（Ｄ）はステップ５４の状態を示す図である。

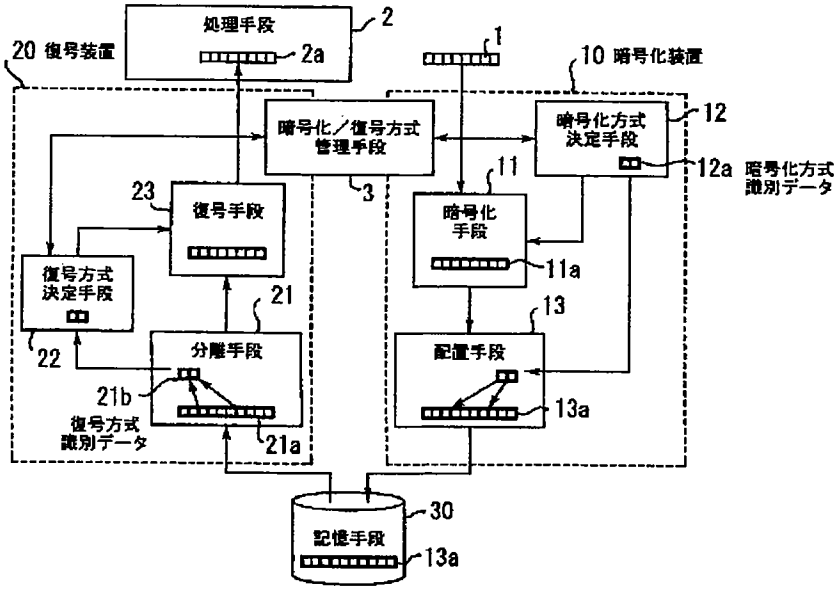
【図１８】従来のソフトウェアの保護を図った情報処理装置のブロック図である。

【符号の説明】

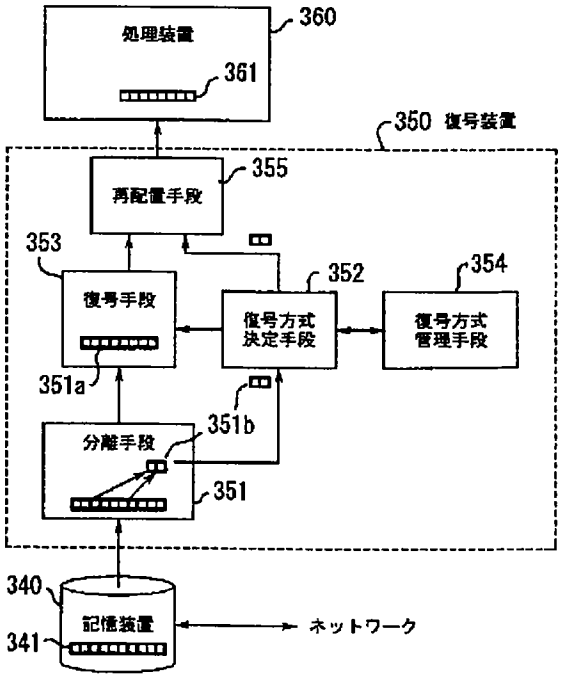
１　暗号化対象データ
２　処理手段
３　暗号化／復号方式管理手段
１０　暗号化装置
１１　暗号化手段

１１ａ　暗号化データ
１２　暗号化方式決定手段
１２ａ　暗号化方式識別データ
１３　配置手段
１３ａ　暗号化データ
２０　復号装置
２１　分離手段
２１ａ　復号対象データ
２１ｂ　復号方式識別データ
２２　復号方式決定手段
２３　復号手段
１１１　ＭＰＵ
１１２　暗号化／復号装置
１１３　鍵テーブル
１２１　メインメモリ
１２２　Ｉ／Ｏインターフェース
１２３　補助メモリ
１３１　システムバス

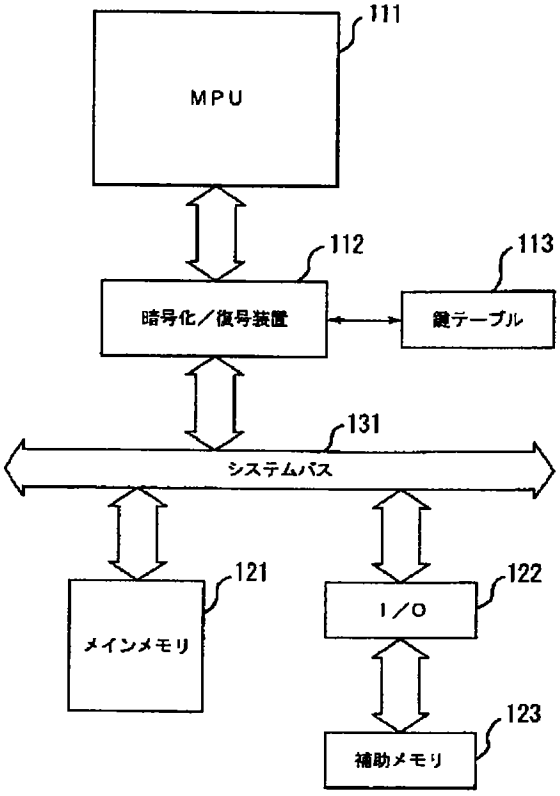
【図１】



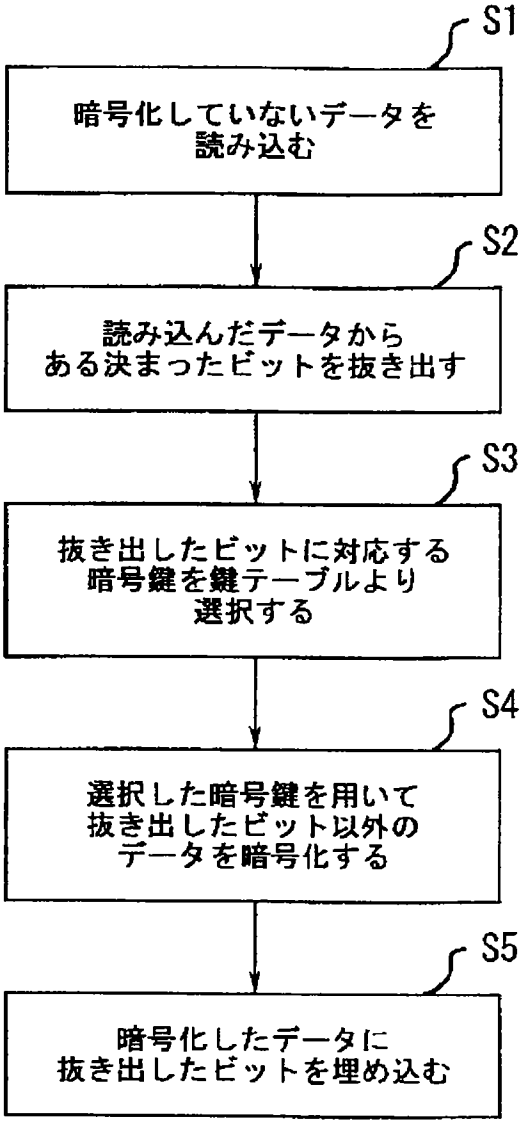
【図１３】



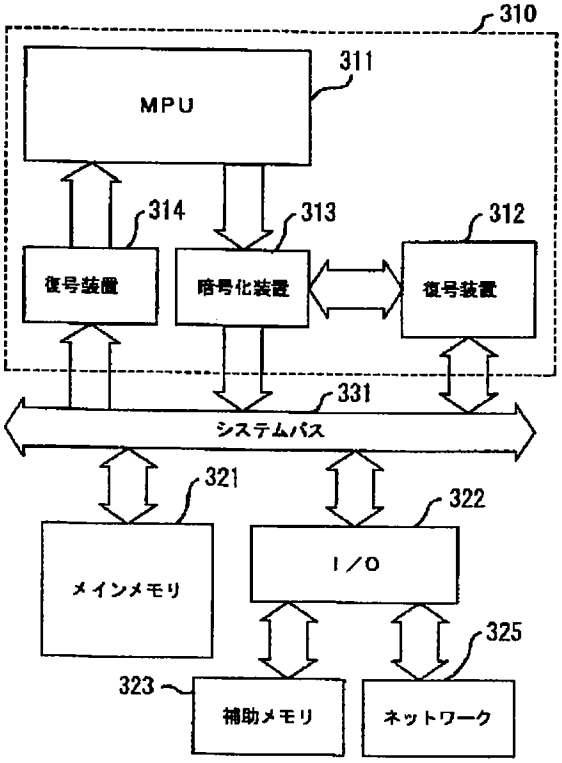
【図２】


111
MPU
112
113
暗号化／復号装置
鍵テーブル
131
システムバス
121
122
メインメモリ
I／O
123
補助メモリ

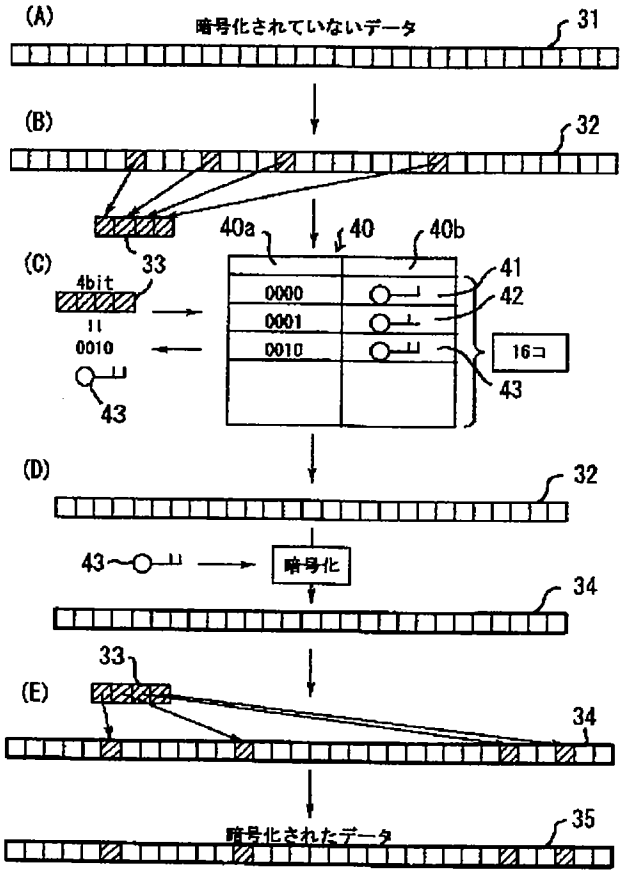
【図３】


S1
暗号化していないデータを
読み込む
S2
読み込んだデータから
ある決まったビットを抜き出す
S3
抜き出したビットに対応する
暗号鍵を鍵テーブルより
選択する
S4
選択した暗号鍵を用いて
抜き出したビット以外の
データを暗号化する
S5
暗号化したデータに
抜き出したビットを埋め込む

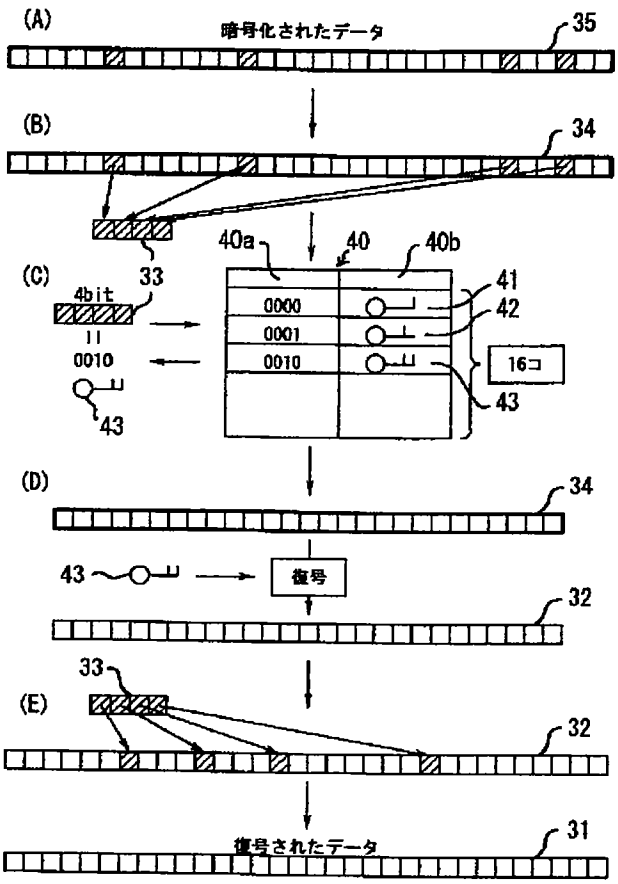
【図１２】


310
311
MPU
314
313
312
復号装置
暗号化装置
復号装置
331
システムバス
321
322
メインメモリ
I／O
325
323
補助メモリ
ネットワーク

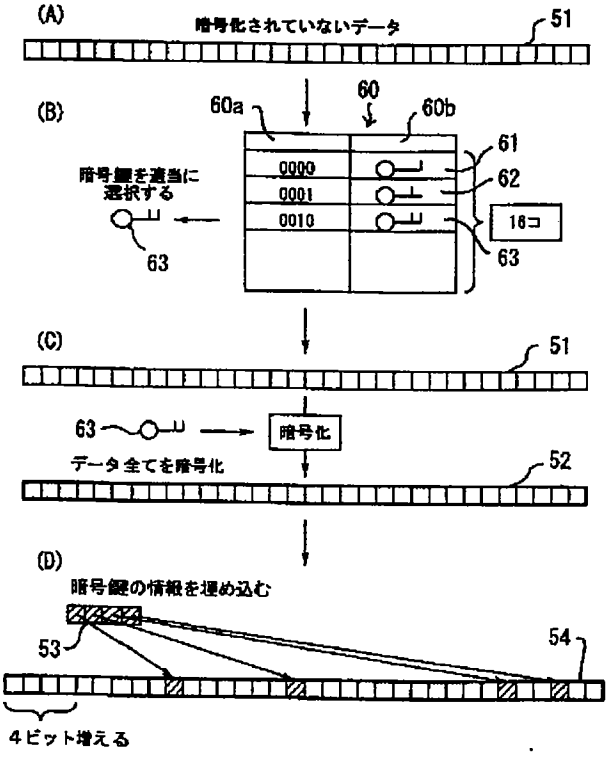
【図４】


(A)
暗号化されていないデータ
31
(B)
32
40a
40
40b
(C)
4bit
33
0010
43
0000
0001
0010
41
42
16コ
43
(D)
32
43
暗号化
34
(E)
33
34
暗号化されたデータ
35

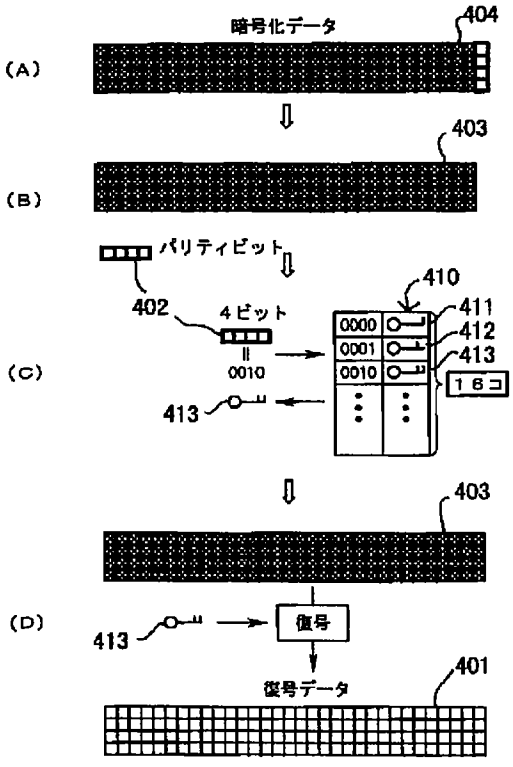
【図６】


(A)
暗号化されたデータ
35
(B)
34
40a
40
40b
(C)
4bit
33
0010
43
0000
0001
0010
41
42
16コ
43
(D)
34
43
復号
32
(E)
33
32
復号されたデータ
31

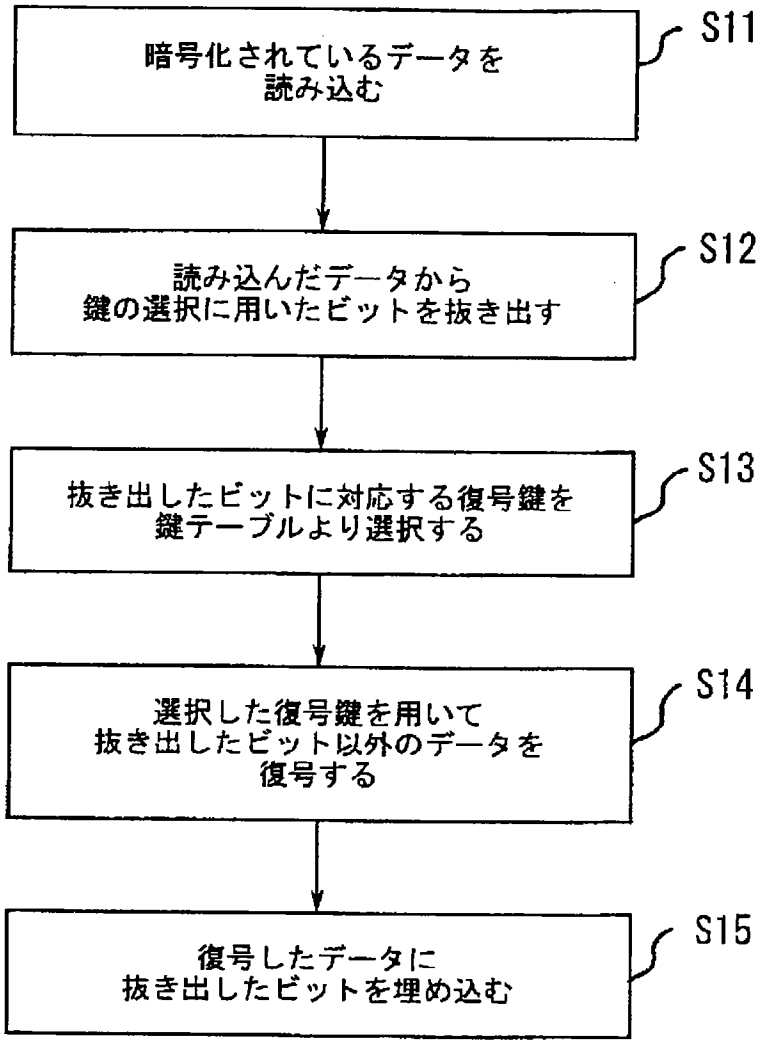
【図９】


(A)
暗号化されていないデータ
51
(B)
60a
60
60b
暗号鍵を適当に選択する
63
0000
0001
0010
61
62
16コ
63
(C)
51
63
暗号化
データ全てを暗号化
52
(D)
暗号鍵の情報を埋め込む
53
54
４ビット増える

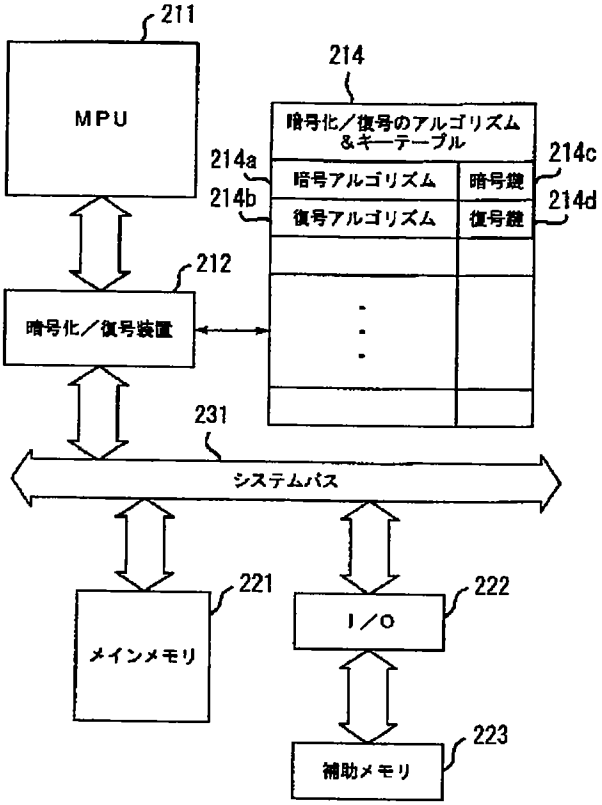
【図１７】


暗号化データ
404
(A)
403
(B)
パリティビット
402
４ビット
0010
410
411
412
413
0000
0001
0010
１６コ
(C)
413
403
(D)
413
復号
復号データ
401

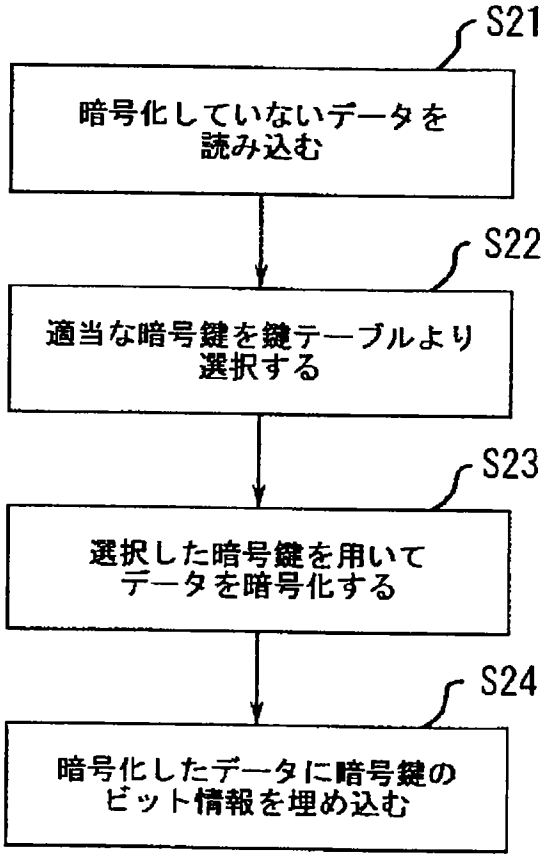
【図５】


暗号化されているデータを
読み込む
S11
読み込んだデータから
鍵の選択に用いたビットを抜き出す
S12
抜き出したビットに対応する復号鍵を
鍵テーブルより選択する
S13
選択した復号鍵を用いて
抜き出したビット以外のデータを
復号する
S14
復号したデータに
抜き出したビットを埋め込む
S15

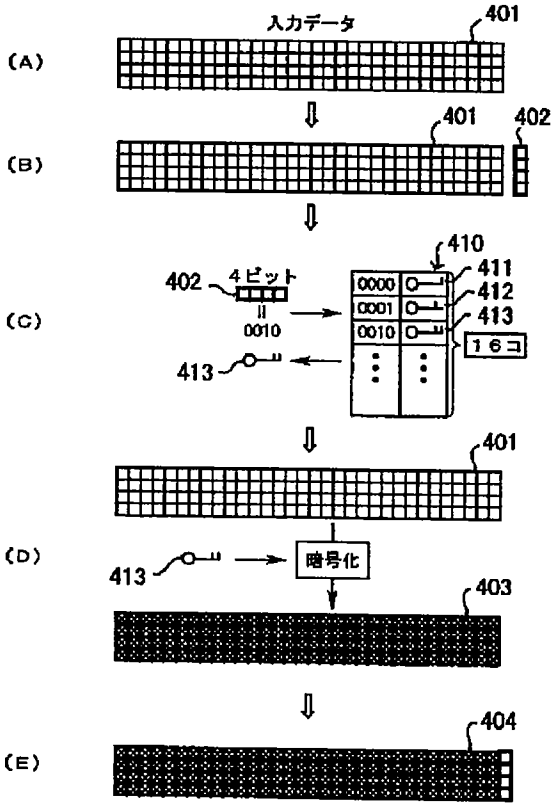
【図７】


211
MPU
214
暗号化／復号のアルゴリズム
&キーテーブル
214a
214c
暗号アルゴリズム
暗号鍵
214b
214d
復号アルゴリズム
復号鍵
212
暗号化／復号装置
231
システムバス
221
メインメモリ
222
I／O
223
補助メモリ

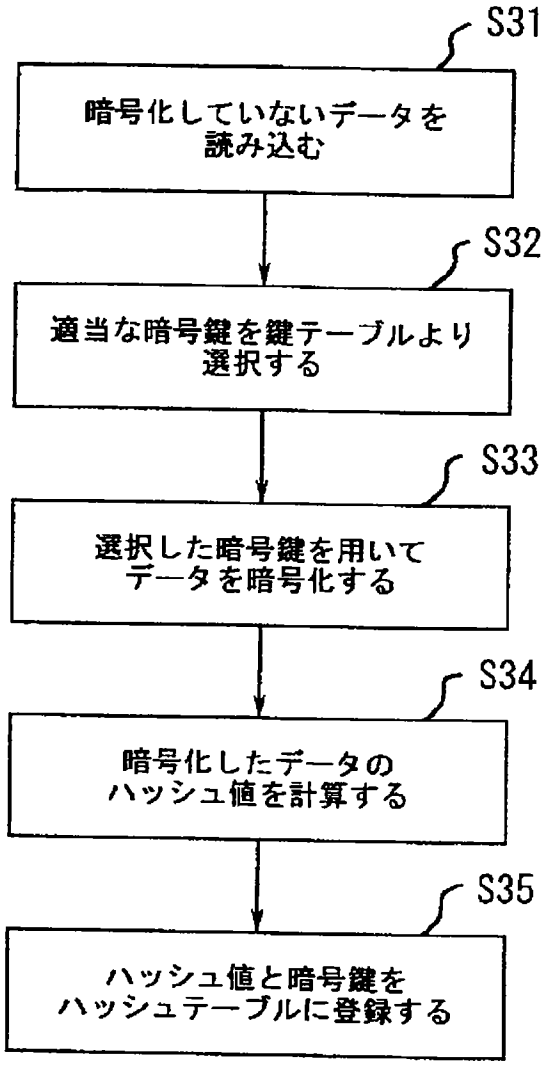
【図８】


S21
暗号化していないデータを
読み込む
S22
適当な暗号鍵を鍵テーブルより
選択する
S23
選択した暗号鍵を用いて
データを暗号化する
S24
暗号化したデータに暗号鍵の
ビット情報を埋め込む

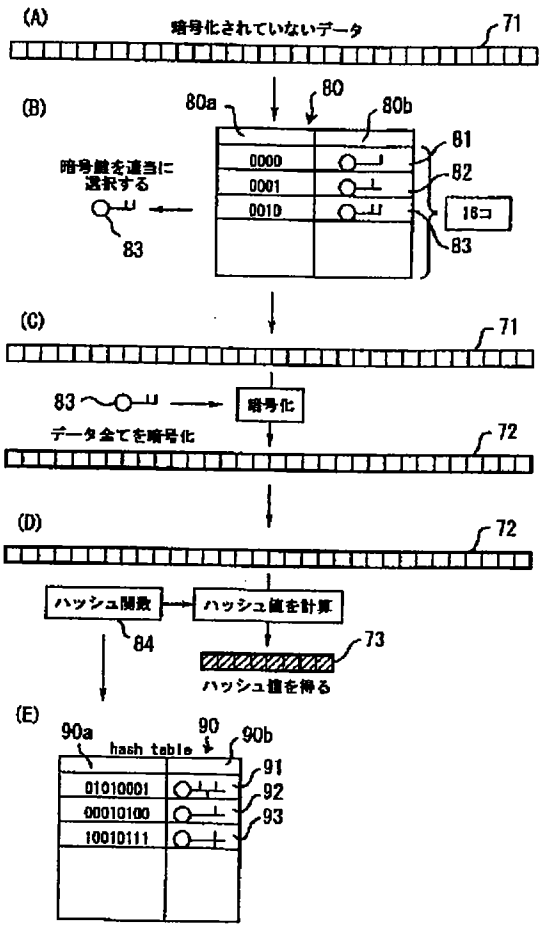
【図１５】


(A)
入力データ
401
(B)
401
402
(C)
410
402
4ビット
0010
411
412
413
0000
0001
0010
１６コ
413
401
(D)
413
暗号化
403
(E)
404

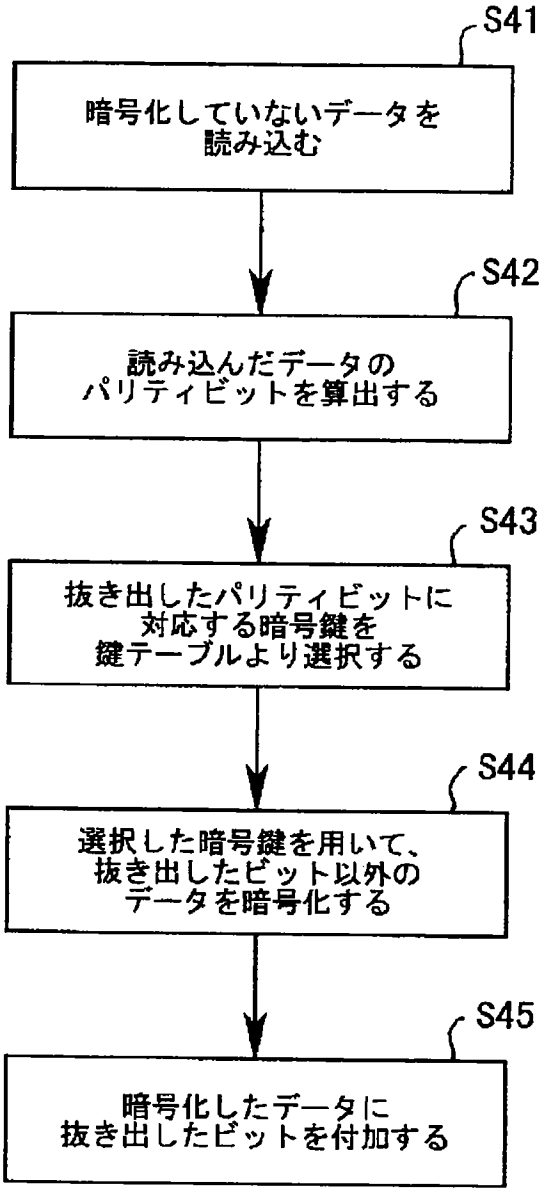
【図１０】


S31
暗号化していないデータを
読み込む
S32
適当な暗号鍵を鍵テーブルより
選択する
S33
選択した暗号鍵を用いて
データを暗号化する
S34
暗号化したデータの
ハッシュ値を計算する
S35
ハッシュ値と暗号鍵を
ハッシュテーブルに登録する

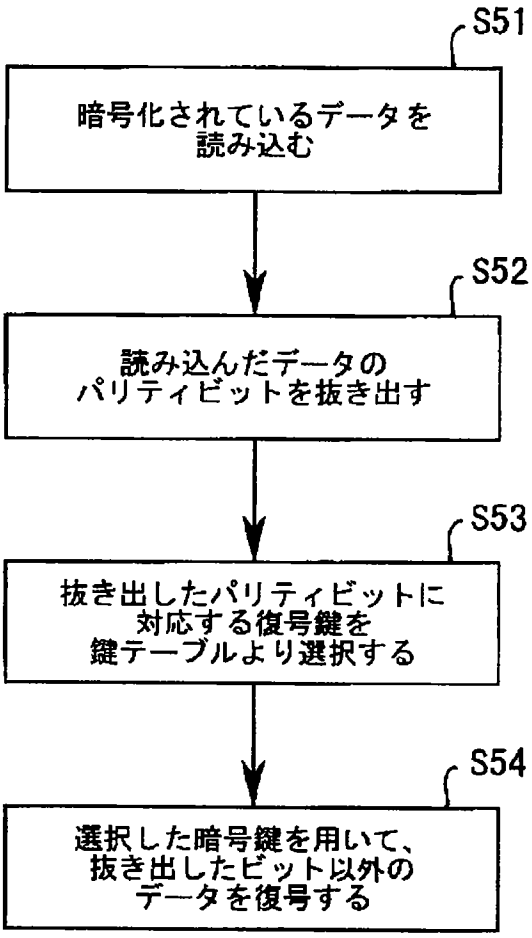
【図１１】


(A)
暗号化されていないデータ
71
(B)
80a
80
80b
暗号鍵を適当に
選択する
0000
0001
0010
81
82
16コ
83
83
(C)
71
83
暗号化
データ全てを暗号化
72
(D)
72
ハッシュ関数
ハッシュ値を計算
84
73
ハッシュ値を得る
(E)
90a
hash table
90
90b
01010001
00010100
10010111
91
92
93

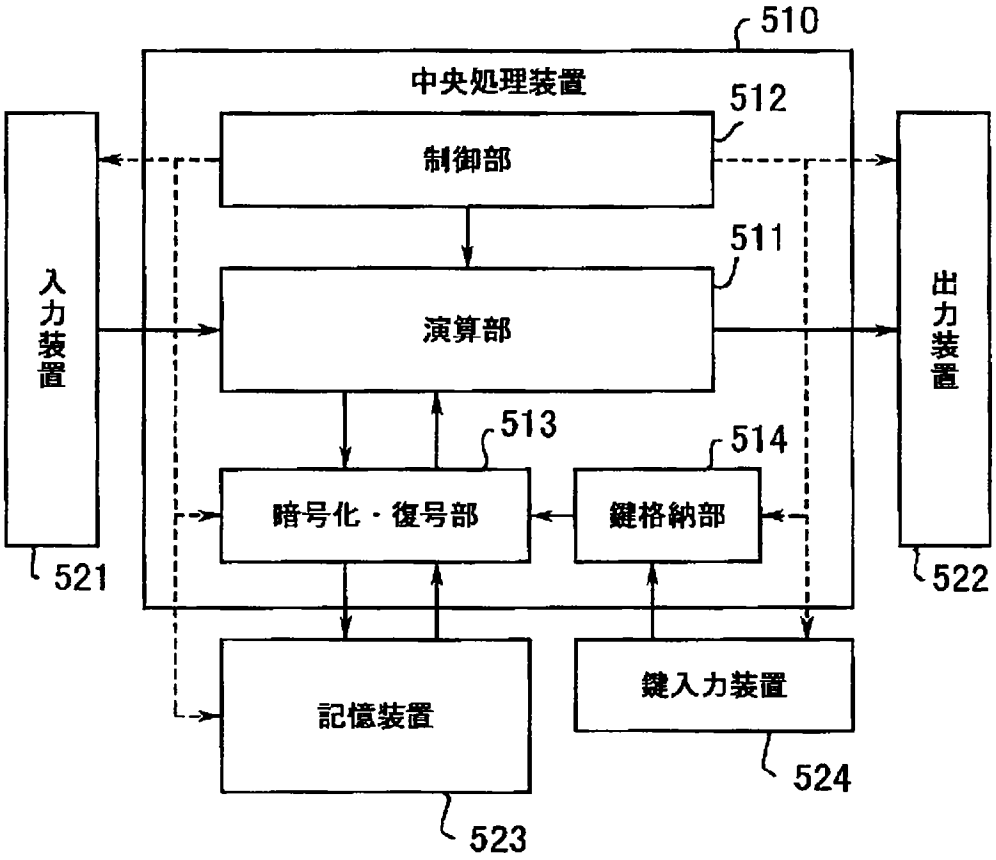
【図１４】


S41
暗号化していないデータを
読み込む
S42
読み込んだデータの
パリティビットを算出する
S43
抜き出したパリティビットに
対応する暗号鍵を
鍵テーブルより選択する
S44
選択した暗号鍵を用いて、
抜き出したビット以外の
データを暗号化する
S45
暗号化したデータに
抜き出したビットを付加する

【図１６】


S51
暗号化されているデータを
読み込む
S52
読み込んだデータの
パリティビットを抜き出す
S53
抜き出したパリティビットに
対応する復号鍵を
鍵テーブルより選択する
S54
選択した暗号鍵を用いて、
抜き出したビット以外の
データを復号する

【図１８】


510
中央処理装置
512
制御部
511
演算部
513
514
暗号化・復号部
鍵格納部
入力装置
出力装置
521
522
記憶装置
鍵入力装置
523
524

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１４年１０月２５日（２００２．１０．２５）

【公開番号】特開平９－２７０７８５
【公開日】平成９年１０月１４日（１９９７．１０．１４）
【年通号数】公開特許公報９－２７０８
【出願番号】特願平８－１８０４５３
【国際特許分類第７版】
H04L 9/14
G09C 1/00 630
H04L 9/08
【ＦＩ】
H04L 9/00 641
G09C 1/00 630 B
H04L 9/00 601 B

【手続補正書】
【提出日】平成１４年７月１６日（２００２．７．１６）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正内容】
【発明の名称】　情報処理装置及び情報処理方法
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　入力されたデータを、識別データと暗号化対象データとに分離する分離手段と、
前記分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、
前記決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成する暗号化手段と、
前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。
【請求項２】　入力されたデータを暗号化する暗号化装置を有する報処理装置において、
暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を選択する選択手段と、
前記選択手段により選択された暗号化方式を用いて前記入力されたデータを暗号化し、暗号化データを生成する暗号化手段と、
前記暗号化手段により暗号化された暗号化データを、所定の関数に入力して関数値を計算する計算手段と、
前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記計算手段により得られた関数値に対応付けて格納する復号方式記憶手段と、
を有することを特徴とする情報処理装置。
【請求項３】　暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、
前記決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、
前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。
【請求項４】　前記暗号化手段を囲む包囲体に対して外部から物理的な作用を受けると、前記暗号化手段の処置機能を司るデータを消去する安全保護手段を、さらに有することを特徴とする請求項１、請求項２、又は請求項３のいずれか１項に記載の情報処理装置。
【請求項５】　前記決定手段により決定される暗号化方式を変更する変更手段をさらに有することを特徴とする請求項１、請求項２、又は請求項３のいずれか１項に記載の情報処理装置。
【請求項６】　識別データが復号対象データ内の所定の位置に配置された入力データを、前記識別データと前記復号対象データとに分離する分離手段と、
前記分離手段が分離した前記識別データに応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する決定手段と、
前記決定手段で決定された復号方式を用いて、前記復号

対象データを前記復号対象データと同ビット数に復号する復号手段と、
前記識別データを、前記復号手段で復号されたデータ内の所定の位置に配置する配置手段と、
を有することを特徴とする情報処理装置。
【請求項７】　入力された暗号化データを復号する復号装置を有する情報処理装置において、
前記暗号化データを、所定の関数に入力して関数値を計算する計算手段と、
前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記関数値に対応づけて格納する復号方式記憶手段と、
前記計算手段により算出された関数値に対応する復号方式を前記復号方式記憶手段内から選択する復号方式選択手段と、
前記復号方式選択手段で選択された復号方式を用いて、前記暗号化データを復号する復号手段と、
を有することを特徴とする情報処理装置。
【請求項８】　前記復号手段を囲む包囲体に対して外部から物理的な作用を受けると、前記復号手段の処理機能を司るデータを消去する安全保護手段を、さらに有することを特徴とする請求項６又は請求項７のいずれか１項に記載の情報処理装置。
【請求項９】　前記決定手段により決定される復号方式を変更する変更手段を、さらに有することを特徴とする請求項６又は請求項７のいずれか１項に記載の情報処理装置。
【請求項１０】　データの暗号化及び暗号化データの復号を行う暗号化装置及び復号装置を有する情報処理装置において、
入力されたデータを、識別データと暗号化対象データとに分離する入力データ分離手段と、
前記入力データ分離手段が分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、
前記暗号化方式決定手段により決定された暗号化方式を用いて暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成する暗号化手段と、
前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置する配置手段と、
前記配置手段により前記識別データが配置された暗号化データを格納する記憶手段と、
前記記憶手段に格納された前記識別データが配置された暗号化データを、識別データと暗号化データとに分離する分離手段と、
前記分離手段により分離された識別データに応じて、暗号化方式に対応した復号鍵と復号アルゴリズムとの組み合わせにより特定される復号方式を決定する復号方式決定手段と、
前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを前記暗号化データと同ビット数に復号する復号手段と、
前記復号方式決定手段による復号方式を示す識別データを、前記復号手段で復号されたデータ内の所定の位置に配置する再配置手段と、
前記復号手段により復号されたデータの処理を行う情報処理手段と、
を有することを特徴とする情報処理装置。
【請求項１１】　データの暗号化及び暗号化データの復号を行う暗号化復号装置を有する情報処理装置において、
暗号鍵と暗号化アルゴリズムとの組み合わせにより特定される暗号化方式を選択する暗号化方式選択手段と、
前記暗号化方式選択手段により選択された暗号化方式を用いて暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、
前記暗号化手段により暗号化された暗号化データを、特定の関数に入力して関数値を計算する第１の計算手段と、
前記暗号化データを復号する復号鍵と復号アルゴリズムとから特定される復号方式を、前記第１の計算手段により得られた関数値に対応づけて格納する復号方式記憶手段と、
前記暗号化手段により暗号化された暗号化データを格納する記憶手段と、
前記記憶手段に格納された暗号化データを、特定の関数に入力して関数値を計算する第２の計算手段と、
前記第２の計算手段により算出された関数値に対応する復号方式を、前記復号方式記憶手段内から選択する復号方式選択手段と、
前記復号方式選択手段で選択された復号方式を用いて、前記暗号化データを復号する復号手段と、
前記復号手段により復号されたデータの処理を行う情報処理手段と、
を有することを特徴とする情報処理装置。
【請求項１２】　予め復号鍵と復号アルゴリズムとが特定されている暗号化データが入力されると、入力された暗号化データを復号する既知方式復号手段をさらに有し、
前記暗号化手段は、前記既知方式復号手段で復号されたデータも、暗号化対象データとして暗号化することを特徴とする請求項２、請求項３、請求項１０、又は請求項１１のいずれか１項に記載の情報処理装置。
【請求項１３】　入力された暗号化データが暗号化された際の暗号化方式と異なる暗号化方式により、前記復号手段が復号したデータを暗号化する別方式暗号化手段を、さらに有することを特徴とする請求項６、請求項７、請求項１０、又は請求項１１のいずれか１項に記載

の情報処理装置。

【請求項１４】　入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する決定手段と、

前記決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化する暗号化手段と、

を有することを特徴とする情報処理装置。

【請求項１５】　復号対象データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する決定手段と、

前記決定手段で決定された復号方式を用いて、前記復号対象データを復号する復号手段と、

を有することを特徴とする情報処理装置。

【請求項１６】　入力された暗号化対象データのパリティビットの値に応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定する暗号化方式決定手段と、

前記暗号化方式決定手段により決定された暗号化方式を用いて前記暗号化対象データを暗号化し、暗号化データを生成する暗号化手段と、

前記暗号化手段により生成された前記暗号化データを格納する記憶手段と、

前記記憶手段内に格納された前記暗号化データのパリティビットの値に応じて、復号鍵と復号アルゴリズムとから特定される復号方式を決定する復号方式決定手段と、

前記復号方式決定手段で決定された復号方式を用いて、前記暗号化データを復号する復号手段と、

を有することを特徴とする情報処理装置。

【請求項１７】　入力されたデータを、識別データと暗号化対象データとに分離し、

分離した識別データに応じて、暗号鍵と暗号化アルゴリズムの組み合わせにより特定される暗号化方式を決定し、

決定された暗号化方式を用いて前記暗号化対象データを暗号化し、前記暗号化対象データと同ビット数の暗号化データを生成し、

前記暗号化データの暗号化に用いられた暗号化方式を示す識別データを、前記暗号化データ内の所定の位置に配置することを特徴とする情報処理方法。

【手続補正３】

【補正対象書類名】明細書

【補正対象項目名】０００１

【補正方法】変更

【補正内容】

【０００１】

【発明の属する技術分野】本発明はソフトウェアの保護機能付情報処理装置及び情報処理方法に関し、特に処理が行われたデータを逐次暗号化する暗号化装置を有するか、処理を行うべき暗号化データを逐次復号する復号装置を有するか、あるいはそれらの双方を有する情報処理装置及び情報処理方法に関する。

【手続補正４】

【補正対象書類名】明細書

【補正対象項目名】００２９

【補正方法】変更

【補正内容】

【００２９】本発明はこのような点に鑑みてなされたものであり、コンピュータのメモリの管理方法に依存せずに、少ない計算量の暗号アルゴリズム及び簡単な鍵管理により暗号強度の高い暗号化データを得る暗号化装置を有する情報処理装置及び情報処理方法を提供することを目的とする。